AD NUMBER

AD509378

CLASSIFICATION CHANGES

TO: unclassified

FROM: confidential

LIMITATION CHANGES

TO:

Approved for public release, distribution unlimited

FROM:

Distribution authorized to DoD only; Operational and administrative use; 23 Apr 1970. Other requests shall be referred to Naval Research Laboratory, Washington, DC, 20390.

AUTHORITY

NRL ltr, 24 Aug 1998; NRL ltr, 24 Aug 1998

NRL Report 7033
Copy No. [redacted]

The I of CNI: Some Identification Problems and Their Relation to Communications and Navigation

[Unclassified Title]

WALTON B. BISHOP

Security Systems Branch
Electronics Division

April 23, 1970

NAVAL RESEARCH LABORATORY
Washington, D.C.

SECURITY

This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. The transmission or revelation of its contents in any manner to an unauthorized person is prohibited by law.

CONTENTS

ABSTRACT

(U) The military and civilian requirements for identification are examined to determine what sort of communications and/or navigation techniques may, or might, be used to satisfy them. A tentative updated list of identification requirements and a draft of characteristics that an electronic system needs in order to satisfy them are provided.

PROBLEM STATUS

This is an interim report; work is continuing on other phases of the problem.

AUTHORIZATION

NRL Problem R01-45
A36533/652/69F15-222-602

Manuscript submitted December 3, 1969.

THE I OF CNI: SOME IDENTIFICATION PROBLEMS AND THEIR RELATION TO COMMUNICATIONS AND NAVIGATION
(Unclassified Title)

1.0 INTRODUCTION

For at least twenty years, concern has been expressed about the proliferation of electronic equipment that military aircraft must carry. There has been a consistent effort to reduce the size, weight, and power requirements of each electronic system or device, but only recently has there been any serious effort to combine the functions performed by two or more electronic "black boxes" into a single one. Simultaneously with efforts to reduce size, weight, and power, efforts have been made to increase performance capabilities, reliability and maintainability. Although much progress has been made, it is generally agreed that much more can, and should, be done in the electronic field to enable high performance aircraft to accomplish their missions more effectively. Functions that can be combined to advantage should be (1). Unnecessary equipment should be dispensed with. New capabilities must be provided in some areas, and costs should be reduced where such reductions will not jeopardize performance.

In response to a request from the Naval Air Systems Command, the Naval Research Laboratory has been studying the feasibility of combining the Communications, Navigation, and Identification (CNI) functions that electronic equipment in aircraft are required to perform. One result of this study has been the discovery that the requirements for C, N, and I functions are not clearly defined although some are documented, and many presumed requirements are not being satisfied by current equipment. This report describes what has been learned by the author to date concerning the I function that must be a part of any CNI system. Similar efforts concerning the C and N functions separately are expected to follow. These three efforts should aid in determining the best way in which all required C, N, and I functions can be satisfied. In short, this report describes the Identification or "I" functions that: (a) *must*, (b) *should if possible*, or (c) *need not* (perhaps cannot) be performed by a CNI system. For convenience, the capital letters C, N, and I are used in place of the words Communication, Navigation and Identification, respectively, throughout this report.

Part 2.0 of this report enumerates all of the required I functions that have been labeled as such in reports studied or discussions held to date. The intended purpose of each function is described in this section without regard to whether or not the function belongs in a CNI system. Parts 3.0 and 4.0 describe all of the places where I functions might be needed and explains why a CNI system should be expected to perform in many, but not all, of these places. Part 5.0 describes the different types of I systems that might be used to accomplish the required functions described in Part 2.0. Part 6.0 describes some of the important characteristics that a CNI system must have if it is to satisfy I requirements. Part 7.0 names specific systems that are in use, under development, or being studied for the performance of I functions and indicates, insofar as possible, their current availability status or references where such information can be found. Part 8.0 lists some of the major problem areas that require further effort if a CNI system capable of satisfying all I functions is to be developed. Part 9.0 provides a brief summary of the conclusions reached in this study of I requirements.

2.0 PURPOSES

The uses of I systems may be classified under the broad headings of military and nonmilitary. However, since military operations in peacetime are often the same as, or very similar to, civilian operations, military uses may be assumed to include nonmilitary uses. A separate listing is provided here for convenience in discussing how the various functions are to be performed. Those I functions that are useful for both military and nonmilitary purposes are listed as nonmilitary because they can, in general, be developed in the competitive civilian market. No security classification problems are associated with their production. The military purposes listed should thus be interpreted as military only.

2.1 Military

The general purpose of an I system for the military departments* is to provide a means of identifying enemy, neutral, and friendly vehicles, objects, stations, and/or personnel

1. With assurance adequate to justify release of weapons,
2. At ranges commensurate with tactical situations,
3. Rapidly enough for tactical needs,
4. Under all weather conditions,
5. Under all traffic conditions,
6. In spite of enemy attempts to inactivate (e.g., jam) the system, and
7. Regardless of any equipment an enemy may possess (including duplicates of all that we possess).

The I system that provides the above functions must also

1. Interface with all data processing and/or display systems in use,
2. Be invulnerable to enemy attempts to "spoof" the system, i.e., cause it to identify an enemy as a friend, and
3. Not be susceptible to exploitation by an enemy.

It should be noted that the above statement concerning the military purpose of I is little more than a rewording of what has been stated as the primary function of an IFF system in a number of earlier documents (2-4). The ways in which this general I (or primary IFF) function can be accomplished vary tremendously with such factors as what is to be identified, the distance between identifier and identified, the potential loss that can result if an error is made, the types of weapons available, the physical location of the identifier and identified, and the number of identifications to be made per unit of time.

*The first draft of this general statement of the I requirement was prepared at the Naval Electronic Laboratory Center (NELC), San Diego, Calif., by L. Higgins, E. Montalvo, V. Terp, and the author during his visit to NELC in December 1968.

2.2 Nonmilitary

There are nonmilitary needs for ways of establishing the true identity of all sorts of items. The most outstanding of these is for a way of identifying *people*. Since this I need probably antedated all of the others, a listing of some of the techniques applicable may be of interest. The list must include ways of determining and comparing all physical characteristics and capabilities such as height, weight, color, sex, facial structure, deformities, scars, tattoos, fingerprints, voice, habits, writing characteristics, signature, address, and numbers assigned to bracelets or necklaces. Photographs provide one of the most convenient ways of identifying people, but the process of identifying them was going on long before photography was invented. Also, various types of coded information may be used to identify people. For centuries, cryptographic messages have been particularly valuable in establishing the true identity of fellow spies. Identifying animals by a brand or a numbered tag so that they cannot easily be stolen or so that they can be returned to their home is also a well-known I technique, and brand names placed on merchandise also provide a means of I. All sorts of appliances and machines carry manufacturer's serial numbers that can be used to identify them. The numbers on plates attached to automobiles (or painted on them) provide one of the most common I techniques in use today, but it is of little value unless the number can be read. The numbering technique has been extended to aircraft by painting the tail of each aircraft with its own number or letter and number combination. Since the aircraft is usually too far away from an air traffic controller for the number to be read, some other means of determining the "tail" number is needed.

The nonmilitary I functions associated with aircraft are essentially in a class by themselves. Air traffic controllers depend heavily upon the data provided by existing systems, and new capabilities are continually being requested. The aircraft identifier is usually at a ground station. However, the aircraft I functions would be very similar if he were on a ship. The nonmilitary needs for identifying one aircraft from other aircraft or from space vehicles have not yet been defined, but as aircraft and space vehicle performance increases and the need for identifications at greater distances develops such needs can be expected.

Nonmilitary aircraft I systems are needed for at least the following purposes (5):

To enhance radar targets and thus improve tracking capabilities (I of those blips or spots on a radar scope that really represent aircraft);

To determine the tail number assigned to an aircraft that produces a detectable signal on a radar (or secondary radar) scope (aircraft Personal I when nothing is known about the aircraft's tail number; called Active Readout PI);

To determine the exact position of an aircraft having a particular tail number (aircraft Personal I) when an aircraft having a particular number is expected (called Passive Decode PI);

To determine the altimeter reading (altitude) of all aircraft within range of the air traffic controller (I of radar signals that represent aircraft at each altitude increment);

To determine the existence of an emergency in any aircraft (I of the radar signal that represents an aircraft in distress);

To provide status reports concerning equipment, fuel, etc., that may have bearing on air traffic control, e.g. ATCRBS* reply code 7600 is used to indicate aircraft radio communications failure (aircraft status I);

To locate the exact origin of radio communications (Special Position I, SPI, or I of Position, I/P);

To provide a means of preventing collision between aircraft, i.e. to provide an effective collision avoidance system, (I of aircraft on collision courses and I of paths that are safe from collisions**).

3.0 CATEGORIES***

All possible places where I functions may need to be performed are included in the following five categories where the vehicle, object, station, and/or person to be identified is considered as the category heading.

3.1 Air

3.1.1 Air-by-Ground (AG)†††

The Air-by-Ground (AG) subcategory of airborne I is by far the most comprehensive. It must be a major part of any CNI system. It includes the I of all types of airborne objects by both fixed and mobile ground stations, and even by an individual soldier or marine with an antiaircraft weapon. Both the military and nonmilitary I functions listed in the preceding section concerning the I of aircraft must be performed by all major ground installations, and the military I functions must be performed before any ground-based weapon can be released to destroy an airborne target.

3.1.2 Air-by-Water (AW)†††

The word *water* is used here to indicate that the identifier is on the surface of water, usually the ocean. In general, surface ships can use the same I techniques that are suitable for ground-based identifiers. Except for the environmental conditions and space limitations imposed on equipment, the AW and AG I subcategories may be combined. This subcategory must also be included in any CNI system.

3.1.3 Air-by-Air (AA)†††

The I of airborne objects by airborne identifiers is the most difficult-to-satisfy subcategory of the I function. Size, weight, and space limitations prohibit use of some techniques that are quite effective for ground- or ship-based systems. The AA I subcategory is another vital part of any CNI system.

---

*ATCRBS is the acronym for Air Traffic Control Radar Beacon System. NATO countries denote this system by SSR for Secondary Surveillance Radar.

**This function has thus far been omitted from ATCRBS as described in Ref. 5. A number of ways of providing collision avoidance have been suggested (6,7).

***The subcategories in this part are noted as follows:

†††Major subcategory: Must be included in CNI System.

††Supplementary subcategory: Further study needed.

†Excluded subcategory: Excluded from current CNI efforts due to lack of need or lack of capabilities.

3.1.4 Air-by-Space (AS)††

Identifiers located in space vehicles have certain advantages, due to their physical location, over airborne identifiers. Their relative inaccessibility, however, serves as a severe disadvantage in other respects. Information obtained by or relayed via satellites may be of considerable importance in the performance of functions required by other subcategories of the I function, and hence must be included in all serious CNI studies.

3.1.5 Air-by-Undersea (AU)†

It would be very convenient for a submarine to have the capability of identifying aircraft without first coming to the surface or allowing an antenna to surface. This capability is not well enough developed to be included in any anticipated CNI system at present, however.

3.2 Space

Most space vehicles can be identified by their position or orbit if this can be observed accurately enough. This observation is usually aided by radio and/or radar transmissions. The ease with which such transmissions can be used and the uses made of space vehicle identifications vary considerably with the position of the identifier.

3.2.1 Space-by-Ground (SG)††

Intercontinental Ballistic Missiles (ICBM's) and various space vehicles may have very similar, or even identical, trajectories during large portions of their spacepaths. Those ground stations which have a capability to counter ICBM's need a means of identifying them. As long as only two countries have space vehicles (and ICBM's) the problem of separating "theirs" from "ours" can probably be handled by simply keeping track of all of ours. Those remaining must then be theirs. However, this does not tell us which of theirs are dangerous. This is an important I function, and it is hoped that an effective CNI system may help solve it. However, current technological developments do not warrant including this function on the same time scale, or with the same emphasis, as some of the others. It must be included in CNI studies, however.

In addition to the ICBM problem, there is a Space-by-Ground I problem for small (or very small) ground-based units concerning the use of I information relayed to them via space vehicles. There must be a means of assuring that such relayed information is authentic. The problem of putting this relayed information in usable form is also quite difficult. A thorough study of the possible use of satellites to relay I information is needed before final decisions are made concerning CNI equipment development.

3.2.2 Space-by-Water (SW)††

The statements made concerning the SG I subcategory apply equally well here. The SW subcategory must also be studied carefully.

3.2.3 Space-by-Air (SA)††

The I of space vehicles by airborne identifiers may be more effective than by ground- or water-based identifiers because of the longer range capabilities and low r-f attenuation in the upper atmosphere. However, the restrictions on space and weight tend to work against development of this capability. The relative survivability of airborne and space vehicle identifiers must also be compared with that of water and ground identifiers. (A surfaced submarine is considered here as a water-based identifier.) The SA I subcategory also should be included in CNI studies.

3.2.4 Space-by-Space (SS)†

Although there certainly must be some consideration of using space vehicles to identify ICBM's or other dangerous enemy space vehicles, it does not seem appropriate to include this I category in current CNI studies. It may have to be included at a later date, however, if technological developments call for it.

3.2.5 Space-by-Undersea (SU)†

If surfaced submarines are excluded (they may be considered along with water-based identifiers), current technology does not permit the I of space vehicles from under the sea. Consequently the SU I subcategory must be excluded from CNI studies.

3.3 Ground

The identification of objects located on the ground varies greatly with the location of the identifier. Thus the distinction between subcategories is more pronounced here than in some of the other categories.

3.3.1 Ground-by-Air (GA)†††

Airborne identifiers need to identify certain ground stations for navigation purposes, others for avoidance, and still others for weapons deployment. In general, this subcategory has I requirements that are quite similar to those of the AA subcategory. Hence it too belongs in any CNI system.

3.3.2 Ground-by-Space (GS)††

Just as for the AS subcategory, this subcategory may aid in the performance of other I subcategory functions. It must, therefore, be included in CNI studies, even though there may be only marginal interest in Ground-by-Space I per se.

3.3.3 Ground-by-Ground (GG)†††

The I function for this subcategory must operate over very short distances for troop activities, and in some applications the equipment must be man-portable. Commonality between equipment for the I subcategories of GA, AG, and GG appears to be

essential if a man is going to be able to carry all equipment required. Also, commonality between I equipment used by heavy land vehicles and man-portable I equipment is needed. Hence, the GG subcategory of the I function also belongs in the CNI system.

3.3.4 Ground-by-Water (GW)†††

Precise N should suffice for most of the I functions where fixed ground stations are concerned. Any bombardment of mobile ground targets by waterborne units is usually guided by airborne identifiers (spotters) who require GA I capabilities. The GA identifications require a C system in order to reach a waterborne identifier. Thus, we see that the GW subcategory is a very important part of a CNI system even though the actual identifications are made in another subcategory.

3.3.5 Ground-by-Undersea (GU)†

The long-range weapons carried by submarines are suitable for use only against targets whose exact geographical position has been determined. The I problem for this subcategory thus becomes only a navigation problem for both the submarine and its weapon. The GU subcategory provides no I functions to be satisfied in the CNI system.

3.4 Water

3.4.1 Water-by-Air (WA)†††

This subcategory of the I function includes essentially the same requirements as the GA subcategory, and hence it too can be satisfied by whatever satisfies the GA subcategory, provided allowances are made for the different environment. It also is a necessary part of any CNI system.

3.4.2 Water-by-Space (WS)††

Water-by-Space I may prove to be of considerable value in the future, as space technology progresses. WS I capabilities may also aid in the accomplishment of other I subcategory functions just as the AS and GS I capabilities may do. Further study of the WS I subcategory is needed.

3.4.3 Water-by-Water (WW)†††

This subcategory of I functions may be accomplished largely by relaying information from AW or SW I systems. However, there will always remain the problem of surface ship I when no air or space cover is available. Hopefully, the techniques developed for AA I functions, and perhaps for GG I functions, will be equally applicable to this subcategory. The WW subcategory of I functions must be included in the CNI system even though equipment developed for other purposes *may* be capable of performing all required functions. As a general rule, equipment developed for one environment does not automatically work well in another.

3.4.4 Water-by-Undersea (WU)†

Submarines are very much in need of an effective means of identifying surface ships without surfacing to do so. This category of I will have to be left out of current CNI studies, however, because insufficient progress has been made toward a means of performing WU I.

3.4.5 Water-by-Ground (WG)†††

When unidentified ships approach land, the groundborne identifiers need to detect and identify them before they get close enough to inflict damage. A WG I system with N facilities is needed to determine the exact location of identified objects, and C facilities are needed to relay the information to the groundborne identifiers. Thus the WG subcategory is similar to the GW subcategory in that it is an important part of a CNI system but uses I information from another subcategory.

3.5 Undersea

The identification of submerged submarines is a severe unsolved problem. Increased efforts are needed on it. Some of the techniques used in other I subcategories may eventually aid in the solving of this problem, but for the present, all five of the following undersea subcategories must be excluded from the CNI efforts.

1. Undersea-by-Air (UA)†
2. Undersea-by-Space (US)†
3. Undersea-by-Water (UW)†
4. Undersea-by-Undersea (UU)†
5. Undersea-by-Ground (UG)†

3.6 Summary of I Subcategories Essential to CNI

A review of all 25 subcategories of the I function shows that an effective CNI system for use during the next twenty years must satisfy the requirements of at least the following nine subcategories: AG, AW, AA, GA, GG, GW, WA, WG, and WW. Concentration upon the more difficult AG and AA subcategories must not cause the severe size and weight restrictions of the GA and GG subcategories to be overlooked, and the problems inherent in using a common system for nine different purposes must not be neglected. A CNI system that satisfies less than these nine I subcategories only postpones the real problem of integrating functions and in fact may serve to add at least one more black box to the current inventory without replacing any. The review also shows that the AS, SG, SW, SA, GS, and WS subcategories of the I function must be studied carefully to see how functions in these subcategories can contribute to the accomplishment of the nine major subcategories. The remaining ten I subcategories may (or must) be neglected in current CNI studies, but some of them need more research effort independent of the CNI program. The conclusions reached in this part of the report are summarized in Table 1 (p. 42) and illustrated in Fig. 1 (p. 43).

4.0 RANGES

The distance between the identifier and the identified has an important bearing upon the way in which I functions can be performed. Figure 2 illustrates how the electromagnetic spectrum tends to divide I functions into groups according to range. If the identifier is at point A in Fig. 2 (p. 43) on the surface of the earth (either ground or water), then audio signals will reach to some very limited distance; it will be possible to see objects clearly somewhat further, and special infrared transmitters and sensors will usually be able to reach out a bit further than visible light can penetrate. Radar techniques, theoretically, should be able to detect objects as far out as points B and C in Fig. 2, but experience has shown that operational radars cannot detect small targets at this range. However, secondary radars, which use one-way or *direct-mode* transmissions (at frequencies high enough so that they travel in straight lines) instead of reflected signals, can reach out to any point that can be touched by a line segment drawn from point A and not passing through any solid objects. The "straight line" distance from point A to the most remote airborne vehicle (at maximum altitude) that can be reached by these direct mode transmissions is roughly 250 naut mi. Objects that cannot be touched by a line segment from A that does not pass through the surface of the earth are usually said to be over the horizon. In order to reach over-the-horizon objects with high-frequency or straight-line r-f transmissions, signals must either be reflected or relayed. In Fig. 2 the region that can be reached only by such signals is labeled the relayed-mode Region. The region where relayed-mode transmissions can be used includes the regions where direct-mode transmissions and radar signals are effective, just as the infrared region includes the visual region and the visual region includes the audio region. Objects that are not over the horizon from the identifier are sometimes said to be within line of sight, but since it is impossible to see as far as this area extends, the term *direct mode* seems more appropriate as a title. The intermediate region shown in Fig. 2 represents the range of airborne vehicles that are usually kept under close control by an air traffic controller. Automatic aircraft landing systems operate in this range, and while in some systems the range can be increased by the flick of a switch, the functions performed usually change at greater ranges.

Although Fig. 2 has been prepared primarily to show how the AG, AW, GA, and WA I subcategories are affected by range, it also shows the limitations placed on the GG, GW, WG, and WW subcategories, and the maximum direct-mode range for the AA category. An airborne identifier cannot use direct-mode transmissions at ranges greater than the distance between points B and C.

4.1 Audio

The I function at audio ranges has been well developed for centuries. Such techniques (or analogies of them) as the use of code books, code words, pass words, whistling a particular tune, firing guns according to a schedule, and giving a characteristic yell or yodel, are in fact just now becoming feasible at some of the greater ranges through the use of electronics.

Audio signals may be of very great importance in solving future underwater I problems. However, as stated earlier, these I functions must be neglected in current CNI studies.

Except for its historical significance, audio-range I may be neglected in current CNI studies. This neglect does not mean that the capabilities of the human ear to identify

characteristic sounds can be neglected. But the ear will have to be aided by some sort of auxiliary equipment if it is to perform useful identifications in a CNI system.

4.2 Visual

The range at which vehicles or objects can be identified by visual means is unacceptably short. However, when all other means of I fail, it is still necessary to rely on visual I. A good I system should reduce the need for visual I to a minimum, but the realization that this minimum may well be unacceptably large leads to immediate agreement with the conclusion of an earlier study (8) that called for both the use of improved binoculars and the development of better short-range weapons.

There are, of course, a number of communications techniques that can make use of the visible spectrum to accomplish I functions. Morse code by signal lights is a well-known example. The use of coherent light offers some new possibilities, especially at high altitudes and in outer space. Visual I techniques are to be neglected in the CNI study, not because they are unimportant, but because they operate essentially independent of other techniques and may thus always be held in reserve.

The human eye, even more than the human ear, will remain one of the major sinks in I systems, but electronic equipment will have to produce characteristic shapes or colors at appropriate positions in various types of displays so that the eye can "read" the I data. Electronic computers can, and should, replace the eye as a sink for some, but not all, I data. The determination of which decisions should be made by man and which by machines is an important problem for CNI systems as well as for many other systems.

4.3 Infrared

There are a number of new developments that make use of the infrared spectrum in identifying objects. Some of these may become very important and may eventually supplement or even become a part of CNI systems. However, due to the precarious state of these developments and the extremely high security classification of some of them, they must be excluded from current CNI studies. The decision to exclude infrared techniques from CNI systems may have to be reconsidered, however, as technology advances.

4.4 Intermediate

Automatic aircraft landing systems operate over the intermediate-range torus, cross sections of which are illustrated in Fig. 2. In principle, the same r-f techniques (radar and secondary radar) can operate at much greater ranges, but the I functions to be performed at greater ranges are not the same. The I functions to be performed in the intermediate range are ordinarily considered as nonmilitary, because, ideally, no unfriendly aircraft should ever be allowed to penetrate this zone of defense. But since this ideal situation is not always realized, and since military aircraft must often comply with civilian air traffic controller's instructions, the intermediate region I functions are of considerable importance to all. The importance of determining such I data as tail number, altimeter reading, position, type of aircraft, speed, and current status have been well documented in "Aviation Week and Space Technology" (9) as well as in the "U.S. National Standard for the IFF Mark X (SIF) Air Traffic Control Radar Beacon

System (ATCRBS) Characteristics" (5). The intermediate range I functions must be performed by any CNI system. It should be noted that this intermediate range covers everything from audio range out to the maximum range of aircraft automatic landing systems.

4.5 Radar

The torus beyond the intermediate region throughout which radar is effective is one of the most important regions where any CNI system must make identifications. It is in this region that so-called military IFF systems have been designed to operate most effectively. These systems are improperly named, for IFF is an abbreviation of "I Friend or Foe," and thus far the IFF systems can identify only friends. The assumption that those who are not friends are foes is not always valid. It is primarily for this reason that there have been many objections to IFF (really "Friend I") systems now in use and/or being produced. These Friend I systems have a number of other disadvantages, which are explained in the following section, but they have one major *advantage* which, paradoxically, has prevented them from performing their primary I function effectively, although it has promoted their use. The Friend I systems that make use of interrogations which elicit replies from friends have a range advantage over radars because they make use of direct r-f transmissions in both directions, whereas radars depend upon reflected signals. Thus the Friend I systems can be used to track friendly aircraft of all sizes out to the maximum range of the direct mode as shown in Fig. 2. It is this tracking capability that is being used most extensively by both military and nonmilitary ground- and water-based installations today. Also, these same Friend I systems are now being used to collect detailed information concerning aircraft for the use of air traffic controllers (5). The almost continuous use of these Friend I systems as tracking aids and air traffic control aids interferes with their use to identify targets detected by radar, and further, the fact that such information can be obtained without radar has led to a downgrading of the importance of radar and may very well have contributed to aircraft collisions. The ATCRBS (secondary radar) is being used more and more in place of radar rather than as an aid to radar. In such cases, aircraft without transponders do not appear on the air traffic controller's scope.

The importance of radar to an I system cannot be overemphasized. Radar provides the only means of detecting a nonradiating enemy aircraft at ranges great enough to permit effective defensive action. The Friend I systems (and there are a number of possible types) all require effective radar and the correlation of identified friends with displayed radar targets.

There are several efforts under way that make use of radar data in an attempt to actually identify *enemy* aircraft as such. (See Part 7.2.1.) To date, however, these efforts have not brought forth a practical Enemy I system. Some of the limitations of such Enemy I systems are discussed in Part 5.2.1.1.

The Friend I system, which assumes that all unidentified vehicles are enemies, and the Enemy I system, which assumes that all unidentified vehicles are friends, both tend to neglect the problem of identifying neutrals. A neutral vehicle may be attacked either because it fails to respond properly to a Friend I system or because it resembles a known enemy vehicle that an Enemy I system can recognize. Although in a hot war it is not likely that neutrals will remain long in a battle area (one side or the other is almost certain to attack them), the consequences of attacking a neutral vehicle can be quite severe. There are a number of operational procedures that can be used to reduce the danger of attacking neutrals. These same procedures can also serve as a reserve way

of identifying friends whose equipment has failed. The use of operational procedures for I is cumbersome, capable of handling only a small number of vehicles at a time, and somewhat dangerous to use. The operational procedures usually involve both C and N facilities, however, so they fall directly in the area to be studied under the heading of CNI.

The military problem of identifying low-flying aircraft is particularly acute in the radar range region. Aircraft flying at very low altitudes may very well first be detected by radar when they are within what is labeled the intermediate range in Fig. 2. Such pop-up targets must be identified very quickly. Consequently, a rapid-acting I system throughout the intermediate range region is essential, and such a system is *desirable* throughout the entire radar range region. The problem of correlating aircraft identified by direct r-f transmissions (either one way or two way) with targets detected by radar exists throughout the entire radar range region.

4.6 Direct Mode

The torus throughout which direct-mode transmissions are effective includes the torus of the radar range region (which of course includes the intermediate region) and usually extends to a considerably greater distance than radar range. It is hoped that new radar developments may eventually reduce the difference between the radar and the direct-mode transmission ranges to a negligible figure, especially for aircraft having a large radar cross-sectional area. In the meantime, there will continue to exist some unique I functions to be performed by direct-mode transmissions at greater ranges than those at which radar systems are effective. The Friend I systems that might function in the direct-mode region beyond radar range are sometimes called cooperative I systems because the object to be identified must cooperate with the identifier in order to be identified.

During World War II and for some time thereafter, documented I requirements invariably called for the I of targets immediately after their detection by radar (2-4). The need for I of friendly aircraft that were beyond radar range had not yet been recognized. The use of airborne radars had been recognized as an important way of extending radar coverage, however, and along with this went a requirement for airborne I systems.* Direct r-f transmissions from aircraft also are usually effective over greater ranges than are airborne radars. Figure 3 (p. 44) drawn to the same scale as Fig. 2, illustrates this difference. Figure 3 shows how a high-flying airborne identifier (at point A′) can use radar and/or direct-mode transmissions to reach the over-the-horizon region that is beneath the normal radar range region of a ground station at point A. The direct-mode range of an airborne identifier is considerably greater than that of a ground- or water-based identifier. This range should be adequate for most I functions, so it is doubtful if the use of a satellite-based identifier can be justified on the basis of the increased range it might provide.

It is now well recognized that there are some advantages in being able to detect and identify friendly aircraft that are beyond radar range (or below the radar-range region), whether enemy aircraft can be detected there or not. Direct-mode airborne transmissions can be used to accomplish this function. In the direct-mode region shown in Fig. 3, the requirement for exceedingly rapid identifications may be relaxed somewhat beyond radar range. There still exists the requirement to correlate identifications made, with targets

*The documentation of this AA I requirement has appeared and disappeared from time to time during the past 20 years, as money has become more and less plentiful.

appearing on some sort of display even though the display does not show radar targets at these ranges. It should now be clear that the I part of a CNI system should be capable of operating at all direct-mode ranges, but the manner in which the I functions are to be performed may vary somewhat with range.

4.7 Relayed Mode

The relayed-mode region shown in Fig. 2 includes all points that a line segment drawn from the identifier A cannot reach without passing through the surface of the earth. The term relay must be interpreted broadly here, for it is meant to include all things that either an active or a passive relay station might do. Thus, the relay station may include such capabilities as a radar with communications facilities for relaying all surveillance data to a remote position, or it may simply pass along messages from one terminal to another.

Airborne radars have been used in large aircraft for some time to extend the range of radar surveillance beyond the horizon of ground- or water-based stations. As radar surveillance range has been extended, the range at which identifications need to be made has been automatically extended too. Now, satellite technology has further increased communications and surveillance capabilities and has simultaneously provided some convenient aids to navigation.

Figure 2 shows that the horizon for a ground- or water-based identifier is well within the intermediate-range region and thus much closer than enemy aircraft should be allowed to penetrate. If surveillance and I capabilities could be extended over the horizon as far as direct-mode signals can be used to reach high-flying aircraft, then I functions could be performed at a more leisurely rate and defense systems could be made far less penetrable. Relay stations located in high-flying aircraft are capable of providing this extension. Satellite-based relay stations could extend the surveillance and I capabilities much further, but at considerably greater cost.

4.8 Summary of Ranges Essential for CNI

A CNI system must be capable of performing I functions from audio ranges out to the maximum direct-mode ranges shown in Fig. 3. CNI studies must determine both the maximum and the minimum ranges over which the relayed mode is suitable for accomplishing I functions, whether such stations should be airborne or in space, or possibly both, and exactly how direct- and relayed-mode capabilities can be made to work together. Again, the capabilities of radar or other surveillance techniques have a strong bearing on how I functions should and/or can be performed.

5.0 TYPES

There are a number of ways in which types of I systems might be defined. We might, for example, say that there are only two types: cooperative and noncooperative. Cooperative I systems would then include all those that require cooperation from the unidentified* (the object to be identified). This definition is not satisfactory because there are so many degrees of cooperation possible that it is difficult to say where cooperation, which might even be inadvertent, ceases.

*We use the term unidentified as a noun throughout the remainder of the report.

We might also say that there are Friend I systems, Enemy I systems, and perhaps Neutral I systems. But there would be no clear demarcation lines separating the systems, for a Friend I system may be used to identify enemies "by subtraction" if no neutrals are present, and systems that identify enemies or neutrals may sometimes identify friends as well.

In keeping with the stated general military purpose of an I system (see Part 2.1), its capability to identify enemies, neutrals, and/or friends should be used as a measure of its *quality*. And each type of system should be subjected to the same evaluation criteria.

It is convenient in evaluating the capabilities of I systems to define the types of systems in accordance with whether the identifier and/or the unidentified is active or passive, i.e., whether each sends messages or not, and whether electromagnetic radiation, when present, is omnidirectional or limited to a small directive angle. With this choice of definition for types of I systems, all existing and proposed I systems can easily be classified unambiguously as one or another of the clearly defined types.

5.1 Identifier Passive

There are some military situations where the identifier needs to keep his presence, or at least his exact location, hidden from enemies. In these situations, the identifier must depend upon radiation that originates elsewhere.

5.1.1 Unidentified Passive

The *ideal* type of I system should be capable of performing I functions with no electromagnetic radiation from either the identifier or the unidentified. Visual I systems permit the identifier to identify objects that are illuminated by ambient light, but they have severe range limitations and hence must be considered as last-resort I systems. Even though there are many ways in which the eye can be fooled, a visual I system augmented by optical aids and perhaps independent light sources may still be used as an adjunct to other I (or CNI) systems. Optical aids could at least provide some improvement in the semisuicidal buddy system in which one aircraft is flown close enough to an unknown aircraft to make a visual I, which is then radioed to a buddy who is in position to attack if the unknown is visually identified as an enemy. Radio-frequency electromagnetic radiation from some source other than the identifier or unidentified could, in principle, supplant the ambient (or independent-source) light to provide another "ideal" I system, but no such system has yet been seriously proposed.

5.1.1.1 Enemy Identification (EI)

The "ideal" type of I system described above works equally well in identifying enemies, neutrals, or friends, but it is not immune from spoofing! An enemy can easily make himself appear to be a friend or a neutral by using a captured, borrowed, duplicated, or perhaps purchased vehicle. The system that is "ideal" from the radiation or detectability standpoint is thus totally unacceptable for use in situations where avoidance of enemy penetration is essential.

5.1.1.2 Neutral Identification (NI)

The nonradiating I system may be used to identify neutrals in some situations, but it must always be supplemented by other means of I where vital areas are to be protected. The use of operational procedures such as following safe-passage corridors are nearly always required in the I of neutrals. These operational procedures also nearly always depend upon reliable C and N for their success. It is thus in the I of neutrals that a CNI system for the purpose of I first comes into use. Clearly, a CNI system has better I capabilities than any simple I system can have in the I of neutrals.

5.1.1.3 Friend Identification (FI)

The nonradiating I system can be made almost completely immune from the error of mistaking a friend for an enemy. This result can only be achieved, however, at the expense of making the often more costly error of mistaking an enemy for a friend. It is for this reason, as well as because all nonradiating I systems have very limited range capabilities, that this type of I system is unacceptable for military use. The range limitation alone makes such I systems unacceptable for nonmilitary use.

5.1.2 Unidentified Active

I systems in which the identifier is passive but the unidentified is active have some unique I capabilities. There are variations of these systems that can identify enemies, others that can identify friends, and still others that can identify neutrals. In general, identifications made by these systems are as valid, or even more valid, than those made by other types of I systems, but there are some disadvantages that have kept most of them from being accepted for wide usage. The advantages and disadvantages of identifier-active, unidentified-passive I systems can best be explained by describing precisely how they can be used to identify enemies, neutrals, and friends.

5.1.2.1 Unidentified Omnidirective

The identifier-passive, unidentified-active-and-omnidirectional type of I system is much more convenient to use than one in which the unidentified's radiation is directional. An enemy's omnidirectional radiation is easier to intercept, and a friend can produce omnidirectional signals with less difficulty.

5.1.2.1.1 Enemy Identification (EI)

If an enemy produces some kind of electromagnetic radiation at the time we wish to identify him, an electromagnetic radiation detector with direction-finding capabilities can be used to determine the enemy's relative azimuth. Two such detectors within range of the radiating enemy can determine his exact geographical position provided that they know exactly where they are and can communicate with each other. If this communications can be intercepted by enemy forces, then action may be taken by the enemy to turn his radiation off so that we can no longer use it. If the enemy continues to radiate as our detector approaches him, then a radiation-seeking missile can sometimes be used effectively against him. If none of our own forces produce the kind of radiation being produced by an enemy, we can be sure that the radiation comes from an enemy or

from a neutral who is using enemy-type equipment. Some types of enemy radiation may carry information that can be used to identify the source *positively* as an enemy. It is not difficult to understand why most military commanders ask for an I system that will identify enemies positively. Also, very little thought is required to understand why the I techniques that might identify enemies positively as such, and that might even tell what type of vehicle (bomber, fighter, guided missile, etc.) an enemy is using, are seldom mentioned. Contracts to develop I systems designed to capitalize on enemy transmissions are not listed with other contract awards in the newspapers, for all such true Enemy I systems are more effective if the enemy does not know that (or how) they are being used. Most of them become ineffective, or even dangerous to use, very shortly after an enemy knows about them. Thus, any knowledgable discussion of this type of Enemy I would have to bear the security classification of Top Secret. The above discussion is based purely upon the author's conjectures about what *might* be done. Anyone who reads American newspapers (or those of any other major power) could easily arrive at the same conclusions. Any similarity between the Enemy I system described here and what is actually being done by any military power is purely coincidental.

Although the Enemy I system that bases its identification upon enemy radiation may be very valuable at times, it has the severe limitation of being effective only when the enemy permits it to be. Also, even when the enemy provides us with convenient radiated energy, it is not always easy to be *positive* that the radiation is coming from an enemy, and the I system is usually quite difficult to automate.

The identifier-passive, unidentified-active-and-omnidirectional I system is another type of I system that uses C and N data to perform I functions.

5.1.2.1.2 Neutral Identification (NI)

It is clearly to a neutral's advantage to make his identity known to both sides of any conflict. If both sides are trying to conceal their exact locations from their opponents, then the neutral is forced to use the identifier-passive, unidentified-active (and usually omnidirectional) type of I system. This system cannot be depended on to protect a neutral who wanders into what either side in a conflict considers a vital area, i.e., one in which enemy penetration must be prevented. The old procedure of shooting first and identifying later is almost certain to be followed when a neutral penetrates a vital area where those who should identify him are passive, i.e., maintaining radio silence. The identifier-passive, unidentified-active-and-omnidirectional Neutral I system can be effective, however, if properly supplemented with a good N system. The neutral can use his N system to make certain that he stays away from all forbidden areas and his C system to keep all combatants informed of his whereabouts. Once again, we see that C and N data can be used to perform I functions.

5.1.2.1.3 Friend Identification (FI)

An identifier-passive, unidentified-active-omnidirective I system can be used to identify friends with very high assurance, provided that the friends to be identified have sufficiently accurate N capabilities, or provided that all identifiers and all unidentifieds have sufficiently accurate clocks. In both cases a cryptosecure r-f communications system is required. As will be seen by the more detailed descriptions of possible I systems of this type, directive transmitting and/or receiving antennas may be used in some cases to increase capabilities.

5.1.2.1.3.1 Position- and Identity-Reporting, Friend-Identification System

If an aircraft can determine its own position accurately, then this position together with the aircraft's tail number, or other I data, can be transmitted via a cryptosecure communications link to all who need to identify the aircraft. This procedure is a very refined version of the old "whistling in the dark" audio I procedure in that all (enemies as well as friends) may receive these transmissions, although the enemies may not recognize the particular "tune." There are ways of concealing these transmissions, however, by various signal processing techniques, some of which make use of accurate time synchronization. Also, the reporting of position and time may be made in accordance with a time schedule to help deny information to listening enemies. The position- and identity-reporting Friend I system has the advantage of completely concealing the location of all identifiers and forcing an enemy to resort to direction-finding techniques to locate the terminals being identified even if transmitted signals are not well concealed. The system has the disadvantage of requiring omnidirectional (or nearly so) transmissions in all areas whether identifiers really need the identity information or not. There are ways, of course, in which the communications portion of a CNI system could be used to turn this one-way system on and off, but this procedure usually requires an active identifier and hence causes the I system to become the active-identifier, active-unidentified type. Further study of this type of system, sometimes referred to as a precise position reporting system (PPRS)* and its possible impact on CNI development, as well as vice versa, is needed.

5.1.2.1.3.2 Time- and Identity-Reporting, Friend-Identification System

The requirement for an aircraft to report its position can be removed if both the identifier and the unidentified have extremely accurate clocks. The difference between the time reported by an unidentified and the time when the signal reaches the identifier can be used to determine range, and the direction from which the signal came can be used to determine azimuth. If ordinary direction-finding techniques are used for this purpose, every transmission (assuming that they are all omnidirectional) can be used by all identifiers within range for I purposes. If a rotating directional receiving antenna is used by the identifier to determine azimuth, then the unidentified must transmit at a relatively high rate in order to be sure that all identifiers receive enough I messages. The use of a rotating directional receiving antenna has the distinct advantage, however, of providing I data that is exceedingly simple to correlate with radar data.

The C link over which time and identity data are transmitted must, of course, be cryptosecure. Further discussion concerning how the time- and identity-reporting system and the position and identity system might be used as part of a CNI system, or how a CNI system might accomplish such functions is provided in Part 5.2.2.1.1.3.

5.1.2.2 Unidentified Directive

The discussion in Part 5.1.2.1 concerning the identifier-passive, unidentified-active-and-omnidirective applies equally well to the type of I system in which the identifier is passive and the unidentified's radiation is directive. However, the directive transmissions add some severe complications.

*Nomenclature due to NELC.

5.1.2.2.1 Enemy Identification (EI)

If the enemy's radiation is directive it will be much more difficult for us to detect and use to advantage. Otherwise the statements made in Part 5.1.2.1.1 apply.

5.1.2.2.2 Neutral Identification (NI)

It is most unlikely that we or our enemies will be able (or desire) to make use of a neutral's directive radiations to identify him. The possibility exists, however, and may be worthy of consideration if a means of using the identifier-passive unidentified-active-and-directive type of I system is developed for the I of enemies and friends.

5.1.2.2.3 Friend Identification (FI)

An identifier-passive, unidentified-active-and-directive type of I system would have the advantage of making the unidentified friend's radiation more difficult for an enemy to detect. The difficulties involved in providing the required rotating directive antennas on aircraft appear prohibitive at present, however, and the I information concerning friends would be far more difficult to collect and use than the I information coming from the identifier-passive, unidentified-active-and-omnidirective type I system would be.

5.2 Identifier Active

In most situations, both military and nonmilitary, identifications are made only at the request of the identifier. The nonmilitary identifiers certainly do not need to conceal their locations, and very often, there is little advantage to be gained by concealing the location of military identifiers, for the enemy either already knows their exact locations or has other convenient ways of determining them. Although the active identifier may use either omnidirective or directive radiation, there seems to be no point in discussing the identifier-active-and-omnidirective, unidentified-passive type of system. No one has yet invented an omnidirectional radar antenna that is effective, and the identifier-active, unidentified-passive type of I system depends upon reflected or radar-type signals. We shall therefore omit further reference to the fact that an I system in which the unidentified is passive must use *directive* radiation.

5.2.1 Unidentified Passive

The identifier-active, unidentified-passive type of I system is often called a noncooperative I system, for it requires no overt cooperation from the unidentified. One of the earliest systems of this type was the searchlight I system of World War II, where the searchlight and identifier were at the same point. Radar may also be considered as an I system of this type, although it can easily be fooled. Actually, radar is an extremely important counterpart of *all* I systems. We have avoided discussing its function until now, because a *passive* identifier, by definition, could not use radar. We must depend upon radar or radiation-detection devices to warn us of approaching unfriendly objects, and in nearly all cases we must use them also to guide any weapons that we launch for the purpose of destroying enemy vehicles. It is the fact that radar is our chief means of detecting enemy objects and one of our chief means of guiding our weapons toward them which makes

it necessary to correlate all identifications with radar targets. This correlation has, of course, traditionally been accomplished by displaying all I information on the radarscope.

Radar can provide useful I information concerning the speed, altitude, and effective cross-sectional area of unidentified objects with little difficulty. More advanced techniques can provide additional information about objects. In fact, it has been claimed that each target generates its own radar "fingerprint" (10). However, the problem of collecting, storing, and correlating large numbers of radar fingerprints is not simple, and the range at which a clear fingerprint can be collected is not as great as the radar range. However, it is not only the complexity of equipment required and the limited range that makes radar fingerprinting impractical. It is the fact that manufactured equipment, such as jet engines, which produce recognizable radar patterns (or fingerprints) cannot be kept in the sole possession of any one group. Experiences in World War II taught us that we could retain sole possession of equipment of any type for only a very short time after it was put into use (and sometimes not even long enough to put it into use). The dangers inherent in using any type of radar fingerprinting or pattern recognition system for the I of enemies, neutrals, or friends becomes more clear when the I of each is considered separately.

5.2.1.1 Enemy Identification (EI)

The general public has an awesome respect for radar. Whether it is used to enforce speed limits, to measure the distance to the moon, or to identify enemy aircraft makes no difference. Radar has been so successful in some areas that people tend to forget that it does have limitations.

On February 8, 1955, the *Boston Traveler* carried an article stating that interceptor pilots were using hand-held flashlights to illuminate the markings of unidentified aircraft in order to determine if they were enemies. The next day the *Christian Science Monitor*, also published in Boston, described the Army's new Nike Guided Missile Station located on an island in Boston Harbor. This article explained how Nike missiles could outmaneuver contemporary planes. Nothing was said about how the planes that Nike missiles were to be used against could be identified. Figure 4 (p. 44) provides photocopies of these two newspaper articles along with their obvious implication. Since these articles, and the many more like them that have been published since, have brought no comment from the public, we must infer that the public believes that the magic of radar will somehow identify all enemy aircraft.

Starting with Project Sambo (11) in World War II, numerous attempts have been made to use reflected radar signals to identify aircraft, and more recently, missiles. Some success has been achieved with a few experimental systems using this technique, but all such Enemy I systems have the two basic weaknesses mentioned earlier: their range is too short and there is no way to make certain the enemy will use the particular type of aircraft that we expect him to use. He may, for example, capture, buy, or produce an aircraft exactly like one of ours or one of a neutral power, and he may sell (or give) one of his own aircraft to a neutral.

Although we are forced to the conclusion that it is unsafe to depend upon any identifier-active, unidentified-passive system alone for the I of enemies, it would be incorrect to say that no useful data can be obtained from such systems. They might provide useful intelligence information about enemy aircraft and/or missiles, and perhaps they can provide useful information for the computers and whatever else is to be used to recognize an

enemy ballistic missile before it is too late. (The author has access to no classified information concerning how such missiles are to be recognized. The above conclusions are based largely upon newspaper articles and knowledge of previous I problems.)

5.2.1.2 Neutral Identification (NI)

The identifier-active, unidentified-passive I system can be no more effective in identifying neutrals than it is for identifying enemies. If such a system were to be used for both Enemy and Neutral I, the number of aircraft radar patterns (or fingerprints) that would have to be stored and compared would soon become prohibitive.

5.2.1.3 Friend Identification (FI)

There are a few cases where the identifier-active, unidentified-passive I system *might* be used to identify friendly aircraft. If we have made only a certain known number of aircraft having a particular recognizable radar-reflection characteristic, and all can be accounted for, then it is usually safe to assume that aircraft producing such reflections are occupied by friends (until such time as an enemy has duplicated our equipment).

In summary, the identifier-active, unidentified-passive I system is really safe to use only for the short range I of a limited number of particular types of *friends*, and then only for a limited length of time. We have neglected to mention also the fact that recent technology may permit the altering or camouflaging of radar target signatures with some rather obvious consequences.

5.2.2 Unidentified Active

The identifier-active, unidentified-active I systems include all those that make use of challenges (interrogations) and replies. In principle, all such systems are variations of the ancient sentry problem where the sentry upon detecting the presence of an unidentified person (or vehicle) calls, "Halt! Who goes there?" and then asks for the correct reply to a coded question, or a series of correct replies to selected questions. A sentry can usually see who is answering, or at least determine the direction from which replies are coming. Thus, correlating responses with those who are responding is not a serious problem for him. When the unidentified objects are beyond visual range, however, correlation between responses and responders can be a very severe problem. The severity of this correlation problem depends largely upon whether directive transmitters and/or receivers are used by the identifier and/or the unidentified. In the following paragraphs, a terminal is considered to be directive if either the transmitter or the receiver or both at that terminal transmits and/or receives over a narrow beam. In most cases of interest, either both transmitter and receiver at a given terminal are directive or neither is.

5.2.2.1 Identifier Omnidirective

Most standard communications systems today use antennas that provide very little directivity, i.e., their beamwidths are usually between 180 and 360 degrees. These antennas alone cannot tell the identifier the direction from which a response comes.

5.2.2.1.1 Unidentified Omnidirective

An I system in which both the identifier and unidentified are active and both use essentially omnidirective antennas could make use of some existing C and N systems to accomplish important I functions. Since such systems require two-way communications, we cannot expect them to identify an enemy directly unless the enemy chooses to let them do so.

5.2.2.1.1.1 Enemy Identification (EI)

If an enemy should happen to use a doubly active and doubly omnidirective I system to identify his own friends, then we should be able to use his omnidirective transmissions to locate and identify both his identifiers and those being identified by him. If we should learn how to duplicate his interrogations and to recognize his replies, we could interrogate his transponders at will and determine their exact location easily. If he should make his transmissions cryptosecure and authenticated, then we would be forced to use direction finders to locate his transmitters and would be unable to take advantage of his I system any time that he chose to refrain from using it himself. (This aspect is covered more completely in Section 5.2.2.2.1.)

5.2.2.1.1.2 Neutral Identification (NI)

Since neutrals are very likely to possess omnidirective communications receivers and transmitters and are more likely to receive omnidirective transmissions than directive ones, the doubly active, doubly omnidirective I system is the logical choice to aid in assuring that neutrals observe proper operational procedures; i.e., to advise neutrals as to what actions they should take to avoid being attacked. Since a neutral's safety depends largely upon the accuracy of his navigation, this I system is still another example of I functions being performed by C and N equipment.

5.2.2.1.1.3 Friend Identification (FI)

The position- and identity-reporting I system and the time- and identity-reporting I system, described in Parts 5.1.2.1.3.1 and 5.1.2.1.3.2, respectively, could be improved considerably by the addition of omnidirective messages from identifier to unidentified telling him when and perhaps how to identify himself. The cryptographic synchronization problems could be simplified considerably by such transmissions, and the unidentified could remain quiet (nonradiating) a much larger percentage of the time.

5.2.2.1.2 Unidentified Directive

It would be convenient for the identifier if his omnidirective interrogations could elicit directive responses back to him. Such a system would also benefit the unidentified by reducing the area over which responses might be detected simultaneously. However, since no such system exists or has yet been proposed, we shall not explore its possibilities further.

5.2.2.2 Identifier Directive

The use of a directive active identifier in an I system makes the data collected exceedingly easy to display on a radarscope and thus provide automatic correlation between I data and the radar targets that produce it.

5.2.2.2.1 Unidentified Omnidirective

The doubly active I systems with directive identifiers and omnidirective unidentifieds are particularly well suited for Friend I. They are so well suited, in fact, that essentially *all* friends can be identified by them. This means that when such I systems are used, the objects that cannot be identified by them as friends can safely be assumed to be either enemies or neutrals. The chief difficulty in using these I systems lies in finding ways to separate neutrals from enemies. These systems are also especially well suited for accomplishing the nonmilitary I functions (5).

5.2.2.2.1.1 Enemy Identification (EI)

In those situations where no neutrals are present, enemies can be identified by subtracting those detected objects that are identified as friends from the total. There are several ways that the absence of neutrals can be assured in the vicinity of any permanent base. Sufficient warnings can be issued to all nonbelligerents to stay away from danger zones, and C and N facilities can be used to assure compliance by the neutrals. In more fluid situations such as those encountered by identifiers on ships and in aircraft, however, the danger of erroneously attacking a neutral can be very real. The proper use of C and N facilities can, even in these more difficult situations, reduce the danger of attacking a neutral to an acceptable level in most situations. If the nonmilitary I capabilities (5) provided by the doubly active I systems with directive identifiers and omnidirective unidentifieds are added to the C and N facilities, then it becomes relatively easy to assure safe passage to any neutral that takes the trouble to file a flight plan.

In addition to identifying enemies "by subtraction," a good I system of this type can easily be made to recognize any serious attempt to jam or spoof the system, and unless the attempt is made in an exceedingly cautious manner, the exact location of the jammer or spoofer can also be determined. More details concerning how this positive enemy I can be accomplished are provided in Part 7.2.2.2.1.

5.2.2.2.1.2 Neutral Identification (NI)

A doubly active I system with directive identifier and omnidirective unidentified is now in use throughout the U.S. for the control of aircraft (5). This Air Traffic Control Radar Beacon System (ATCRBS) accomplishes all of the required nonmilitary I functions listed in Part 2.2 reasonably well, except that of collision avoidance, and it is now being considered for providing that function too (12). Its capabilities in obtaining accurate data from aircraft and correlating this data with radar information makes the problem of developing operational procedures for the control of neutrals in wartime one that can be handled, provided only that the neutral cooperates. Noncooperating neutrals will certainly not remain a problem for long in any conflict, as they will become prime targets for both sides.

5.2.2.2.1.3 Friend Identification (FI)

The doubly active I system with directive identifier and omnidirective unidentified is often called a challenge-reply or interrogation-reply IFF system. The principles upon which friend identifications are made in this system are exactly the same as those used by a sentry who challenges an unidentified person and asks him to give the proper response to a code word or the proper responses to a sequence of code words. An electronic Friend I system, of course, must make identifications much more rapidly than the sentry, and correlation between replies and who is replying cannot be made visually.

In order for any interrogation-reply Friend I system to be effective, some elementary principles must be satisfied:

1. There must be considerably more interrogation-reply pairs than an enemy can possibly collect, store, and use to cause himself to be identified as a friend. Usually there are some constraints upon the rate at which such data can be collected.

2. The code-book or cryptosystem must be such that an emeny cannot use a portion of it to determine the remainder, i.e., it must be such that he cannot determine the key setting to the cryptosystem used by mathematical analysis of collected data.

3. There must be so many possible key settings that an enemy cannot possibly try a sufficiently large portion of them (on a set of known-to-be-correct interrogation-reply pairs) while one setting is in use to have a worthwhile chance of finding the correct one.

The requirement that identifications made must be correlated with radar targets actually arose from the fact that originally, it was the *detected* radar targets which were to be identified as being produced by friends or foes. Now, our I systems usually have greater range capabilities than our radars; so the I systems are required to *detect* friends and identify them simultaneously, and *then* the nonmilitary part of the system is usually required to keep track of the friends that have been identified.

The principles described above are only part of the requirements for a cryptosecure Friend I system. The others are concerned with such things as how key settings are made, how interrogations are selected, when key settings are changed, and the rate at which replies can be elicited by interrogations.

We now return to our consideration of what the doubly active I system with directive identifier and omnidirective unidentified offers, assuming that cryptosecurity is provided. It is within the bounds of our definition for the identifier to use a directive transmitter and omnidirective receiver, or vice versa. Such I systems have been proposed, and a few have actually been used, but they offer few, if any, capabilities that are not provided better by a system where both the transmitter and receiver of the identifier are directive. We shall consider only the latter case.

A directive identifier has the immediate advantage of radiating energy only in the direction that he chooses. Since the unidentifieds have omnidirective receivers and transmitters, the identifier can send messages to all unidentifieds in a particular direction chosen at will, or he can cause his transmit-receive antenna to rotate with, and encompass essentially the same angle as, the radar antenna. Further, if he wishes, he may synchronize his interrogations with the radar pulses so that responses will be received simultaneously with, or immediately after, radar echoes. In both of these cases the interrogation-reply I system is forced to use replies that occupy a very short interval of time so that replies

from two friends who are at the same azimuth and nearly the same distance from an interrogator will not interfere with each other. Since the frequency bandwidth available is quite limited (usually to only two channels) interrogation-reply I systems are capable of transmitting a much smaller number of unique replies than interrogations. This does not limit the number of interrogation-reply pairs that are possible, but it does require an unidentified to answer a number of interrogations correctly before he can be accepted as a friend. The first (historically) and most common method of using interrogation-reply I systems is to mount the antenna used to transmit interrogations and receive replies (the interrogator-responder antenna) physically on top of the radar antenna. This procedure means that identifications must be made during the time that the rotating antenna scans past an unidentified radar target (or past a responding friend who has not yet been detected by radar). In general, the interrogation-reply friend I system is required to identify as friends all responding friendly *unidentifieds* that are within range during a single rotation of the radar antenna. (The fact that some installations may allow as many as four or five antenna rotations to complete this task does not remove the capability requirement.)

The rapidity with which identifications must be made means that high-speed, digital, electronic equipment must actually do the identifying. An operator is required to monitor the equipment and in some cases he may limit the areas where identifications are desired to specific ranges, or azimuths, or both. The operator's main concern however is with those radar targets that are not identified as friends, as described earlier in connection with neutral identifications.

Another variation of the doubly active, identifier-directive, unidentified-omnidirective I system offers the possibility of using the directive transmitter of the identifier to turn on a position- and identity-reporting or a time- and identity-reporting unidentified as described in Parts 5.1.2.1.3.1 and 5.1.2.1.3.2, respectively.

A basic problem associated with all interrogation-reply I systems is to determine a way to keep enemies from using interrogations like ours to elicit responses from our transponders, the receiver-transmitters carried by our unidentifieds. While this problem is one of *authenticating* messages and hence is not entirely new, it is more difficult to solve than the authentication problems found in more conventional cryptosecure C systems. A brief discussion of how this problem can be solved is provided in Part 7.2.2.2.1.

5.2.2.2.2 Unidentified Directive

The ultimate in interrogation-reply Friend I systems would be one that provided directive replies to directive interrogations. Such a system with cryptographically authenticated interrogations and a cryptosecure interrogation-reply pair generator would be exploit-proof, spoof-proof, and exceedingly difficult to jam. There has been some R&D on retrodirective communications systems,* but there is little evidence that an operable system will be ready for use in an I or CNI system soon enough to warrant serious consideration here. (This conclusion might be subject to change if R&D on retrodirective communications is accelerated, or if CNI development takes much longer than anticipated, or both.)

*In particular, by the Microwave Antennas and Components Branch, Code 5250, of the Electronics Division, Naval Research Laboratory, and IBM, Rockville, Md.

If we include the use of modulated retrodirective reflectors by the unidentified as part of an "unidentified directive" active system, then a doubly active, doubly directive Friend I system might be achievable sooner.

The use of modulated retroreflectors for I purposes goes back to World War II (13,14). Their use for communications purposes was suggested by Stockman (15) in 1948, but electronics technology had not advanced far enough at that time to permit much exploitation of the technique (16). There have been numerous rediscoveries of modulated retroreflectors in the last decade (17), and now it seems reasonable to suggest that the feasibility of using modulated retroreflectors for CNI purposes should be thoroughly investigated. The advantages that would accrue from the use of a modulated retroreflector of r-f frequencies are potentially very great, for the reflected signal, which might carry the most critical information, would be highly directive and thus difficult for an enemy to intercept. Earlier studies (16) were forced to reject the use of modulated retroreflectors primarily because

1. There was no convenient way of turning a retroreflector off and thus prevent an enemy's using it, and

2. The modulation frequency range was far too limited, since only the mechanical modulation of reflectors was available.

It is doubtful if either of these reasons is valid today. If solid-state technology can produce sufficiently rapid changes in the conductivity of a surface, or a solid, or a conducting medium, then it is possible to modulate retroreflectors at high frequencies, and if the conductivity can be reduced to zero, then retroreflectors can be turned off! New techniques for preventing enemy use of retroreflectors are also available, provided we have a means of making them retroreflect or not upon demand.

5.2.2.2.2.1 Enemy Identification (EI)

A doubly active, doubly directive I system would have to identify enemies by subtraction, just as other interrogation-reply I systems have to do.

5.2.2.2.2.2 Neutral Identification (NI)

Neutrals could use a doubly active, doubly directive I system as an aid to operational procedures in very much the same way that the present Air Traffic Control Radar Beacon Systems can be used. The neutral would want both sides in a conflict to use the same system, however, and such international agreements are difficult to obtain. The ATCRBS is now being used by the Russians as well as by the U.S. and NATO countries, but at least 15 years were required to achieve the international agreements that make the use of the ATCRBS in NATO possible.

5.2.2.2.2.3 Friend Identification (FI)

A doubly active, doubly directive I system would be almost ideal for friend identification. It could easily be correlated with any radar, or it could be used without radar. Its only difficulty appears to be that the identifier would have to search to locate

unidentifieds wherever radar coverage was missing or inadequate, and would thus be momentarily detectable by an enemy. This procedure could be reversed, of course, if the identifier were required to remain hidden. Doubly-directive communications systems such as required for this I system would also have a large number of other applications in the C and N areas.

6.0 CHARACTERISTICS

A CNI system that is to perform all required I functions should be feasible, adequate, and reliable. Additional requirements, which fall under these categories, are as given below.

6.1 Feasibility

A feasible CNI system is defined as one that uses proven techniques and is implementable, compatible, affordable, and convenient.

1. Uses Proven Techniques. Theoretical predictions alone concerning new techniques are not enough. They must be subjected to proper tests and evaluation before being accepted for use. This does not mean that new techniques cannot be used. It does mean that proven techniques should not be abandoned for new ones until the new ones are really ready for use.

2. Implementable. There must be a reasonable means of putting a CNI system into use. It is not considered reasonable to say that all existing equipment must be removed and replaced by CNI equipment simultaneously throughout the world. The transition from current to future equipment and practices should be evolutionary insofar as possible. A plan for implementation should be a part of any serious CNI proposal.

3. Compatible. The CNI system must be compatible with other equipment in the same environment. For example, the I information coming from a CNI system must be properly coordinated with radar data, and the CNI system must not degrade the operation of any system it does not replace.

4. Affordable. The cost of a CNI system must not be prohibitive. If the cost of developing, testing, and evaluating a new technique is beyond what the prospective users can afford to pay, then that technique must be left out of the CNI system.

a. Cost effectiveness — The long-range cost of the development, production, and operation of a CNI system must be compared with all known alternatives. Only a CNI system that can be shown to be well worth the money, manpower, facilities, raw materials, etc., required to produce, operate, and maintain it should ever be produced.

b. Small size — There is no unused space in modern aircraft where *new* CNI equipment can be placed, and future aircraft are expected to have even less space available. Consequently, if a CNI system is to be developed to perform C, N, and I functions, it must occupy no more than the space now occupied by or planned for separate C, N, and I equipments. The severity of the size restrictions is increased by the fact that during the transition from existing to new systems the CNI equipment must perform both new and old functions in order to remain compatible with any equipment that it has not yet fully replaced. If we define a new parameter that might be called *function* performance

per unit of *volume* occupied (F/V), then a CNI system must possess an F/V at least twice as high as current equipment. The size requirement is perhaps even more severe for the man-portable equipment than it is for airborne equipment. The fact that man-portable CNI equipment must function with airborne equipment for the AG and GA subcategories of I, as well as for some of the C and N functions, must not be overlooked. Note: The fact that the I functions required of man-portable equipment are not as severe as those for airborne equipment offers a possible way of solving this size problem. Because a man can usually afford to identify one target at a time, the equipment can be simpler.

c. Light weight — All airborne equipment should, of course, be made as light as possible, but manborne equipment *must* not exceed a man's carrying capacity. And CNI equipment should be only a *small* portion of the items that a man carries. The solution to this portion of the CNI problem must be coordinated carefully with the Army and the Marine Corps.

d. Low power requirements — Most modern equipment already has rather low power requirements. Further reduction will probably be required, however, in order to permit battery operation of CNI equipment for the lengths of time necessary. CNI power requirements should be less than half that of current equipment if it is to operate without difficulty. This figure also comes from the fact that current capabilities must be maintained while new ones are being implemented.

5. Convenient. The users of a CNI system have a tremendous number of tasks to perform. The CNI system must take little of their time and be exceedingly easy to operate if it is to be successful. Consequently, automatic operation must be incorporated wherever feasible, and the outputs of the system must be in readily usable form. In other words, very careful attention must be given to the human factors involved in the CNI system. The advice of experienced military personnel must be sought and used in determining how the operator's controls and the outputs of the CNI system should be designed.

a. Automatic — A number of I functions can be performed only by high-speed digital electronic equipment. There is no question about the fact that these functions must be automatic, but there are a number of ways in which such automatic operation can be asked for and used. Also, a number of operations can be either automatic or manual. Very often both automatic and manual operation must be available, if only to convince the operator that automatic operation is as good as his own. Also, design for good reliability may call for a manual operational capability to be used in case of certain types of equipment failure.

b. Displayed properly — The problem of displaying I data is very severe for some identifiers. Automatic display on a radarscope is essential for some identifiers. Others may have no radar capability but require a display, or audio output, associated with their weapon-control system. Whatever output is used for the I information emanating from a CNI system, the I data must be in a convenient form for the human operator to use.

6.2 Adequacy

We already have too many inadequate I systems. A CNI system offers the possibility of combining a number of capabilities to provide satisfactory performance of all required I functions. In order to be really adequate as far as I functions are concerned, a CNI system must be satisfactory for all of the joint services, have a multiple-subcategory

capability, a long range and high target capability, a rapid I time, be multifunctional, and have low EA and FR ratios. Additional requirements are given according to category, below.

1. Joint Services. No CNI system will be capable of performing I functions satisfactorily unless it is used by *all* of our military services and by our allies in war. Close coordination among the military Departments on all technical aspects of the design and development, as well as production, of a CNI system is required in order to avoid wasted time and effort on incompatible and/or inadequate systems and to avoid an undesirable duplication of effort on common systems that *are* acceptable.

2. Multiple Subcategory Capability.

a. Air — The CNI equipment carried by an airborne vehicle must provide the C required by identifiers on the ground, on water, and in the air, and it must be capable of identifying unidentifieds on the ground, on water, and in the air in order to satisfy the AG, GA, AW, WA, and AA subcategories of I.

b. Ground — The CNI equipment carried by a man on the ground, or carried by land vehicles, or that located at ground bases must provide the C required by identifiers on the ground, in the air, and on water, and it must be capable of identifying groundborne, airborne, and waterborne unidentifieds in order to satisfy the GG, AG, GA, WG, and GW subcategories of I.

c. Water — The CNI equipment carried by waterborne units (ships and amphibians) must provide the C required by airborne, landborne, and waterborne identifiers and it must be able to identify airborne, landborne, and waterborne unidentifieds in order to satisfy the WA, AW, WG, GW, and WW subcategories of I.

d. Space — The CNI functions performed by space vehicles may aid in the accomplishment of certain required I functions. Such aid is considered supplementary here (see Part 3.0); i.e., it is assumed that a CNI system must be capable of performing all of its required I functions without such aid. However, the use of space vehicles *may* be essential for some C and N functions. If such C and N functions do become a part of the CNI system, then some use of them should certainly be made in accomplishing I functions, particularly those in the relayed-mode region as shown in Fig. 2.

e. Undersea — It is assumed here that submarines will use waterborne equipment or at least antennas at the surface of the ocean to identify waterborne or airborne unidentifieds and to be identified by waterborne or airborne identifiers. This part of the undersea I problem may thus be considered along with those problems in the water category.

It is further assumed that any other means of I used by submarines will be independent of any CNI system. These assumptions are not meant to downgrade the importance of undersea I problems in any way. On the contrary, they tend to show that there has been serious neglect of I problems in the undersea category.

3. High Target Capacity. At certain installations, the CNI system must be capable of identifying large numbers of unidentifieds simultaneously, or almost simultaneously. In particular, permanent ground stations and major waterborne installations must identify all aircraft that come within range of surveillance as often as tracking and guidance facilities require. The exact capacity required depends largely upon the C, N, and storage (or

computer) facilities available. An upper limit to the capacity requirement can be determined by assuming that all aircraft within a radius of 250 naut mi may have to be identified during the time required for a radar antenna to make one complete revolution (about 4 sec).

4. Long Range. In general, the CNI system should be able to identify unidentifieds at least as far away as they can be detected. There are advantages in being able to identify friends and neutrals at ranges greater than that at which enemies can be detected. However, there are some special cases where an I range capability equal to the effective range of the weapons in use can be of great value, and an I capability even at much shorter ranges can be useful if it can make its identifications rapidly enough. (The pop-up targets frequently appear first at very short ranges.) Other studies have shown that where the range capabilities of I equipment are short, some modern weapons are useless. This means that rapidly acting, short-range weapon capabilities must be maintained for the express purpose of functioning with the I equipment available, and that any further increase in weapon range capabilities would be wasteful.

5. Rapid. The time required to make an I should not be greater than the time required for a radar antenna to sweep past a target. In fact, *all* unidentifieds at a particular azimuth but at different ranges should be identified during one look at (or sweep past) them. Multiple looks may be permitted for the I of two or more aircraft at the same range and azimuth but at different altitudes. Hopefully, this situation will not occur often.

The time required for identifications made by man-portable CNI systems must be less than or equal to the human reaction time required to release a weapon after a possible target has been located. There are, of course, some applications where several seconds are available to make identifications, and many installations require rapid identifications only a small portion of the time. This in no way changes the firm requirement for a rapid identification capability in the CNI system.

6. Multifunctional. A CNI system must continue to be at least as multifunctional in accomplishing the nonmilitary I functions described in Part 2.2 as are current "radar beacon" systems, (i.e., the ATCRBS (5). Some of these functions could easily be interpreted as C or N functions, but, since by a type of "grandfather-clause" interpretation they are called I or IFF functions, considering them here is appropriate. The multifunctional capability of the I or CNI system is particularly important in the I of neutrals. It is most unfortunate that the press, radio, and television media today do not distinguish between what is accomplished by the ATCRBS, which is a "secondary radar system," and what is accomplished by radar alone.

7. Low Friend-Rejection Ratio (FR). The friend-rejection ratio (FR) is defined as the number of friends that an identifier rejects divided by the number of friends that he tries to identify. The CNI system must have a FR ratio at least as low as that currently required of military I systems (18). Since this figure is subject to change with the increased capabilities and cost of a friend's equipment, current figures should be used only as a temporary guide. An order of magnitude better than what is now being asked for might eventually be required. We assume here that the value of a friend's life remains constant.

8. Low Enemy-Acceptance Ratio (EA). The enemy-acceptance ratio (EA) is defined as the number of enemies that an identifier accepts divided by the number of enemies that he tries to identify. Several different EA values have been specified as requirements for the I system that is now in production (18). The CNI system must certainly satisfy at

least these values. In general a CNI or an I system must be capable of achieving smaller EA values than it can achieve for the FR values. It is of course the fact that specified EA and FR values must be achieved simultaneously which makes the problem difficult. Automatic data processing becomes essential in any system that is required to achieve low values of FR and EA simultaneously (19).

6.3 Reliability

The usual concepts of what constitutes a reliable system must be expanded in order to describe a CNI system that we can depend on to perform I functions. Some of the following six aspects of reliability are sometimes listed under other headings or are considered as primary objectives in themselves. However, they all contribute to the reliability of I.

1. Spoofproof. We say that if an enemy succeeds in making himself appear as a friend to an I system, then he has spoofed the system. Clearly, this comes under consideration in designing a system to satisfy a specified EA ratio, as described in Part 6.2, item 8. In that section, we pointed out the need for satisfying a low EA criterion. Here, we describe how the criterion can, and we believe must, be satisfied.

a. Cryptosecure — It was concluded more than 20 years ago (20) that only by the use of cryptography could we keep an enemy from using equipment like ours (captured or duplicated) to spoof our I system. It was also recognized very early in the studies of cryptographic I systems that most conventional cryptographic techniques were not adequate for the performance of Friend I. In particular, it was known that

(1) An interrogation-reply type of I system requires an extremely large catalog of interrogation-reply pairs in order to prevent an enemy's collecting and storing enough of them to be able to give the proper response to a large proportion of our interrogations without knowing either the cryptosystem or key setting in use.

(2) An interrogation-reply system in which an enemy can elicit responses to interrogations at will is both dangerous to use in some areas because of the tracking and homing capabilities provided and difficult to make safe from enemy cryptanalysis because an enemy can use the planned-interrogation technique of breaking the cryptosystem. Numerous proposed I cryptosystems have been broken by this technique. (Part 6.3.2.1 describes one way of preventing an enemy's planned interrogations from being answered.)

(3) There must be an extremely large number of key settings for any I cryptosystem so that an enemy cannot try all possible settings with a small number of interrogation-reply pairs that he can easily collect.

(4) True cryptosecurity cannot be achieved in a Friend I system without high-speed digital electronic circuitry. Identifications must be made too rapidly to permit slow procedures that are adequate for some C systems. Fortunately there are, and have been for a long time, many C systems that also require high-speed digital circuitry.

(5) Any I system that uses cryptographic equipment must possess at least two key settings to permit the changing of settings during military operations, e.g., in airborne equipment while in flight. All key settings must be such that they can be set rapidly and conveniently and can be zeroed (returned to the zero setting) automatically when required, or manually when desired. (Attempts to destroy equipment with explosives were proved to be both useless and dangerous during World War II.)

(6) An interrogation-reply Friend I system with a very large number of interrogations and only a few replies has the following advantages:

(a) Its cryptosystem is, in general, more difficult to break by cryptanalysis than most other systems because of the many-one transformations involved.

(b) It can discriminate in range much better than other systems operating with the same r-f frequency bandwidth.

Such a system possesses another characteristic that may be either an advantage or disadvantage depending upon how the system is used: EA and FR criteria can only be satisfied by eliciting several replies from each unidentified. The accept-reject decisions for this system must be made with automatic equipment if EA and FR are both to be made very small (19).

b. Unavoidable — A cryptosecure Friend I system may, in some cases, be spoofed by avoiding the cryptosystem. For example, if a conventional radarscope is used for the display of Friend I information, an enemy might produce display patterns that look like our I information by transmitting properly synchronized signals on the radar frequency. There are a number of other countermeasures that an enemy might use to avoid, or bypass, a cryptographic I system. Some typical countermeasures of this type and countermeasures for them are described in Refs. 19, 21, and 22.

2. Exploitproof. The existence and/or use of a CNI system should not provide the enemy with capabilities that he would not otherwise possess. In other words, he should not be able to exploit the system.

a. Authenticated — An interrogation-reply I system may provide an enemy with a convenient I system and tracking aid if we take no precautions to prevent his interrogations from being answered. There now exists a way of using enciphered time in interrogations so that transponders possessing accurate clocks can recognize authentic friendly interrogations and inhibit responses to nonauthentic ones. Also, it is now possible to use time synchronization along with other I and/or N information (see Parts 5.1.2.1.3.1, 5.1.2.1.3.2 and 7.1.2) to eliminate the *need* for interrogations in a cryptographic I system and simultaneously to assure the acceptance of only *authentic* friendly transmissions from friends. An I system that makes use of C techniques other than that of repeated interrogation-reply pairs also requires authentication of its messages so that an enemy cannot exploit the system.

b. No undesirable side effects — Any I system that radiates may have some undesirable side effects. As a general rule, I equipment should not increase the detectability of either the identifier or the unidentified beyond that which is already available by other techniques. This requirement means that the I function in a CNI system should be accomplished by means of modulation techniques that are equally as sophisticated as those used for the functions considered primarily C or N, and that there should be no unnecessary radiation.

3. Fail-safe. The CNI system that performs I functions should be so designed that any failures which occur will be detected immediately and appropriate action started immediately to compensate for and correct the failures.

a. Automatic testing and warning — The electronic equipment should be tested automatically at periodic intervals to assure its continued reliable operation. The automatic test equipment should indicate the nature and location of failures immediately upon occurrence and, wherever possible, initiate automatic corrective action.

b. Graceful degradation — There must be a number of reserve I techniques available for use in case of any type of equipment failure. Wherever possible, equipment should be designed to operate with only somewhat reduced capability when an electronic failure occurs. In other words, CNI equipment should "degrade gracefully" as failures occur, and not stop operating entirely. This requirement essentially demands the proper use of redundancy, self-testing, and automatic replacement of modules when feasible (23). It should perhaps be noted again here that the I functions *can* be performed by C and N equipment alone when required, even though the identifications may not be made as rapidly or efficiently as desired.

4. Maintainable. CNI equipment will have so many users that it must be maintainable by technicians who have a minimum of technical training.

a. High mean time between failures (MTBF) — All electronic equipment must have mean-time-between-failure (MTBF) ratings at least as high as the C, N, and/or I equipment it replaces. Figures considerably higher than any realized today are needed. Current equipment research and development efforts indicate that a MTBF of 25,000 hours would be a reasonable objective for CNI equipment.

b. Low mean time to repair (MTTR) — When failures do occur in CNI equipment, the time required for repair should be limited to that required to replace the defective module. Locating the defective module should be automatic. A 15-min mean-time-to-repair (MTTR) figure for CNI equipment appears reasonable. The time required to make the replaced module operable again is not considered a part of this MTTR. The repair of modules in electronic shops should also be possible in less than a day in most cases.

5. Interference-Free. The radio-frequency spectrum is rapidly becoming saturated. Care must be taken to keep the various CNI installations from interfering with each other. The use of efficient modulation techniques and information coding, as well as appropriate spectrum assignments, is implied.

6. Difficult to Jam. If an enemy cannot exploit our CNI system, then he is likely to try to jam it. The CNI system should be as difficult to jam as we can afford to make it, and in addition, should be capable of locating the source of any jamming attempts so that the jammer can be attacked by appropriate weapons. When weapons are not available or their use is not permitted, we must be prepared to use alternate means of I to overcome jamming just as we would in case of equipment failure.

7.0 STATUS

The military I functions listed in Part 2.0 are not being performed very well today. However, most of the nonmilitary I functions listed there are being performed reasonably well in continental U.S. and in a few overseas regions. Some effort is being made to develop I equipment of at least five of the types defined in Part 5.0. Only one of these types offers much chance of improvement in the near future, and two additional types may be of considerable value in the somewhat more distant future. The remaining two types being developed can at best offer only very slight aid to the I problem regardless of the effort expended on them. A sixth type appears to offer some new I capabilities if severe technological difficulties can be overcome.

7.1 Identifier Passive

7.1.1 Unidentified Passive

Since the publication of Ref. 8, there has been some renewed effort to improve the visibility of pilots and to design a stabilized pair of binoculars that might be used to increase the range at which other aircraft can be recognized. Visual I, no matter how much improved, will always remain as a "last resort" technique—to be used when all else fails, and then at considerable risk.

7.1.2 Unidentified Active

The use of enemy radiation for I purposes is too highly classified to be discussed here. Appendix D of Ref. 24 describes some work in this area under the title of "TEASER." This description of what is *actually* being done bears the classification Top Secret. Knowledge of this type of work, its successes and its failures, is needed by those who must make decisions concerning research and development in the I area.

7.1.2.1 Unidentified Omnidirective

There is one very important development in the area of Friend I by means of an identifier-passive, unidentified-active-and-omnidirectional type of system. This development, by the Naval Electronic Laboratory Center (NELC) at San Diego, is known by the acronym TIFCO for time frequency correlation (25). The TIFCO system has the following two very useful features that may be needed in a future CNI system:

1. It requires no radiation at all from the identifier.

2. It uses signal processing techniques that permit the use of transmissions from the unidentifieds that are difficult for an enemy to detect. Such signals are referred to as LPI signals, since they should have a low probability of intercept by an enemy.

The principles upon which TIFCO operates may be summarized briefly as follows (24,25):

1. All identifiers and unidentifieds are equipped with precise time pieces and crypto-devices capable of automatically enciphering the time of day.

2. Unidentifieds transmit almost continuous omnidirectional signals having format and frequencies selected by the enciphered time of day.

3. Each identifier uses a directional, rotating antenna to receive the signals transmitted by all unidentifieds within range. The distance between the identifier and unidentified is determined by comparing the deciphered time in each received signal with the actual time. The bearing from identifier to unidentified is determined by the position of the receiving antenna when signals are received.

4. The power level of all transmitted signals is low and the frequency dispersion is wide to make signals difficult for an enemy to receive.

Variations of TIFCO have been proposed for use as a complete CNI system (26), but it is generally agreed that more study and more research and development is needed before any variation could be accepted as a complete CNI system. The means of combining I and N functions, N being provided by an "inverse" form of TIFCO called LISANS for Low Intercept Susceptibility Air Navigation System (27) suggested in the CNI proposal of Ref. 26 appears to offer some advantages over current short-range N systems. Further study of N and C requirements, as well as of I requirements, is needed before any conclusions can be accepted. Only a few experimental models of TIFCO or LISANS equipment have been constructed, but several impressive operational demonstrations have been made with these models* (28).

If, in the final analysis of I requirements, it is determined that identifications must be made with high assurance (i.e., low FR and EA criteria must be satisfied) with no radiation from the identifier, then TIFCO or a reasonable facsimile thereof may be necessary for these identifications. Note: It is already rather well established that it is not necessary for *all* identifications to be made in this manner.

7.1.2.2 Unidentified Directive

There is no existing or proposed I system of the identifier-passive, unidentified-active, and directive type.

7.2 Identifier Active

7.2.1 Unidentified Passive

There have been several attempts to design and develop Identifier-Active, Unidentified-Passive I systems. These systems all use Directive transmitting and receiving antennas. They are sometimes called radar signature or fingerprint recognition systems or simply pattern-recognition systems. In spite of the fact that it was known before the end of World War II that no system of this *type* could ever be of much value for identifying aircraft (11), a considerable amount of effort has been expended on such systems during the past five years (24).

The Target Resolving Information Augmentation Device (TRIAD) developed by Melpar, Inc., Falls Church, Va., has now been abandoned in favor of the Target Recognition through Integral Spectral Analysis Techniques (TRISAT) equipment developed by Scope, Inc., Falls Church, Va., and the Enemy Aircraft Recognition System (EARS), also being developed by Scope, Inc. Since EARS is nothing more than a smaller version of TRISAT and capable of doing even less, we shall limit our discussion to TRISAT.

According to Ref. 29, "TRISAT is a pattern recognition device designed to identify aircraft targets by examining the aircraft engine audio amplitude modulations received on a radar return signal. Two breadboard systems, one for use with a high pulse-repetition-frequency (PRF) radar and the other for use with a low PRF radar, were designed and constructed by Scope, Inc. In support of the program, development tests were conducted at the Naval Weapons Center, China Lake, as reported in NOTS TP 4381."

*Phase 1 of TIFCO was demonstrated in May 1963, Phase 2 in March 1965, and Phase 3 in March 1969.

The avowed purpose of the TRISAT development (29) is "to provide fighter aircraft with an extremely accurate means of positively identifying a target. It must also be emphasized that the need is for a truly effective system. One that carries out a positive identification with a very high confidence level that the aircraft pilot can trust implicitly."

It is difficult to comprehend how any radar pattern-recognition system can ever be used for the positive identification of either enemies or neutrals, for, as mentioned earlier (Parts 5.2.1.1 and 5.2.1.2), enemies and neutrals may exchange equipment or aircraft at will, and an enemy can easily obtain some of our equipment. We repeat here for emphasis what was said in Part 5.2.1.3: The radar pattern recognition type of I system can at best provide positive identification of no enemies or neutrals and only a limited number of friends: those friends who use equipment that we are certain cannot be possessed by either neutrals or enemies. We make no attempt here to evaluate possible uses of TRISAT for anything other than I.

7.2.2 Unidentified Active

7.2.2.1 Identifier Omnidirective

7.2.2.1.1 Unidentified Omnidirective

Most C and N equipment uses either omnidirectional antennas or antennas that cover very large sectors. None of the C or N equipment now in general use has a directivity of only a few degrees, as is common with most of the present equipment used by identifiers. Although there are many ways in which the I function can be performed by means of two-way omnidirectional transmissions, none of them has thus far been used effectively for that purpose. No one has yet made a thorough study of the time and frequency bandwidth required for a two-way omnidirectional I system that must correlate its I data with the position of detected objects on a radarscope. There were a few attempts to use omnidirective antennas at identifier sites in the early days of IFF. All such attempts failed due to either the difficulty of correlating information or the inability to handle as much air traffic as required, or both. Today's high-speed digital circuitry and highly reliable C and N equipment certainly has the capability of performing many needed I functions.

There have been numerous suggestions that the TACtical Air Navigation (TACAN) system, now being used for short-range N (30), and the IFF Mark XII system (31), now being developed for both military and nonmilitary I, should be combined as a first step toward CNI (32,33). These suggestions *appear* to have merit, especially since both systems operate in the L-band, but the exact manner in which the systems should be combined, if indeed they should, requires further study. It seems most appropriate for a CNI group to make this study, since any combination of TACAN and the IFF Mark XII will offer the possibility of providing new C channels.

7.2.2.1.2 Unidentified Directive

The possible uses of an identifier-omnidirective, unidentified-directive I system should be studied to determine if a CNI system might benefit from such a capability. None of the I systems in use or proposed thus far have this capability, however.

7.2.2.2 Identifier Directive

7.2.2.2.1 Unidentified Omnidirective

The IFF Mark XII system now being produced, as well as most of its predecessors (the IFF Mark X (SIF), X, V, . . ., I), is of the identifier-directive, unidentified-omnidirective, interrogation-reply type. Since the IFF Mark XII (31) represents the latest in a long series of evolutionary systems, we shall limit our discussion to it.

The choice of L-band for the IFF Mark XII was made primarily to assure an adequate range capability under all weather conditions. Antenna problems could certainly be simplified, especially for airborne identifiers, if a higher frequency could be used. The proper choice of frequency spectrum for each function must be a part of CNI studies, but we shall drop the subject here and consider only *how* required I functions are satisfied.

The IFF Mark XII is being developed by the DOD-AIMS office at Wright-Patterson Air Force Base, Ohio. The USAF is the executive agent for this development, but all of the armed services are represented on the AIMS Steering Committee; so the development is truly Joint Services. It should be noted that the Naval Research Laboratory and the Air Force Cambridge Research Laboratories worked together for eight years on the research and development that preceded the AIMS program and that in 1957, the Army's Signal Corps Engineering Laboratory joined in the first effort to produce enough experimental models for flight testing (31).

The acronym AIMS comes from ATCRBS IFF Mark X (SIF) Mark XII System. The ATCRBS portion of the AIMS program is supposed to satisfy the nonmilitary I functions listed in Part 2.2. The collision-avoidance requirement is not yet being satisfied adequately, and there is some question as to whether a radio-beacon system can ever succeed in fully satisfying it. Full details concerning the current status of the ATCRBS are provided in Ref. 5. There are some questions about the ability of the ATCRBS to handle all of the air traffic expected in the future. The Department of Transportation (12) is studying this problem, but it should also be a part of the CNI study.

The IFF Mark X (SIF) is very similar to the ATCRBS. In fact, Mode 3/A is common to both, and Mode C soon will be. The Selective Identification Feature (SIF) performs the nonmilitary I functions for military users and in addition increases the military capabilities to use operational procedures for I. The relationships between the ATCRBS and the IFF Mark X (SIF) are described in Ref. 34.

The addition of Mode 4 to the IFF Mark X (SIF), which already includes the ATCRBS capability, makes what is called the IFF Mark XII system. Mode 4 provides some 17 million possible interrogations, (the other "modes" provide a total of only four interrogations at present with two more programmed for future development) and 16 possible replies. Its cryptosystem, which determines the correct reply for each interrogation, has about 10^{21} possible key settings and has been approved by the National Security Agency (NSA) as having adequate cryptosecurity to perform the I functions for which it was designed. Note: This approval does not mean that the cryptosystem is suitable for use in C and/or N systems. A separate mathematical analysis must be made by NSA before any cryptosystem can, or will, be approved for other uses than the ones originally intended.

If properly designed automatic decision devices are used with Mode 4, Enemy Acceptance ratios as low as 0.0001 and Friend Rejection ratios as low as 0.001 can be satisfied. Decision devices can also automatically detect attempts to jam or spoof the system and at least determine the direction from which such signals are coming (19).

The IFF Mark XII system, as now being produced, is primarily for the AG and AW subcategories of I, although there are a few models of AA, WW, and WA equipment being produced. The other five essential I subcategories described in Part 3.0 were considered in the original design of the Mark XII system, however, and their I functions can be provided compatibly when sufficient funds are available for the production of equipment.

The operational requirement which the IFF Mark XII was designed to satisfy (4) calls for the I capability in all nine subcategories listed as essential in Part 3.0. Thus far, there has been no major effort to satisfy all required subcategories of I, but this should not be taken as an excuse to omit them from CNI studies.

The current status of IFF Mark XII equipment production, testing, and use is described in reports from the DOD-AIMS office (35).

The IFF Mark XII system, as now being produced, is somewhat vulnerable to exploitation by an enemy who repeats one of our acceptable interrogations to elicit replies from our transponders. A modification to the IFF Mark XII known as TACIT, for time authenticated cryptographic identification transmissions, has been proposed by NRL (36,37) and is now being considered by the AIMS Steering Committee. TACIT makes use of readily available crystal oscillators to effectively change the cryptographic key setting every second. A remote resynchronization capability with cryptosecurity is also provided. Experimental models of TACIT were flight tested in 1968. Since these tests, TACIT has been modified to provide for the authentication of SIF interrogations as well as those of Mode 4 (38).

A great deal of effort has been spent on making the IFF Mark XII as reliable, easy to maintain, interference-free, and difficult to jam as possible. Studies indicate that further improvements are possible, but not all of them can be afforded. This work is continuing both in the I and CNI programs.

7.2.2.2.2 Unidentified Directive

A two-way active, two-way directive I system would have many advantages over other systems. Some research and development on retrodirective receive-transmit antenna systems is being conducted at NRL* and at IBM**. Although modulated retroreflectors (16) might also be used to provide a two-way directive I system, no effort is being made to develop such a system at present.

8.0 PROBLEM AREAS

Associated with CNI efforts are a number of particularly bothersome administrative problems caused by the many scientific disciplines involved and the fact that any CNI system to be of value must be used by *all* of the military services. We neglect these administrative problems here and discuss only *technical* problems. More particularly, we discuss only those technical problems that are clearly evident from this study of how I functions may be performed. Indubitably there are many more.

*Microwave Antennas and Components Branch, Electronics Division; NRL Code 5250.
**An experimental model of a Retrodirective Communications System was demonstrated at NRL on April 9, 1969 by D. Freedman of IBM, 326 E. Montgomery St., Rockville, Md.

8.1 Antennas

Regardless of *how* the I functions are performed, better antennas are needed. Present antennas that are supposed to provide omnidirectional coverage for aircraft do not provide the coverage well enough, airborne directive antennas are too cumbersome and not directive enough, and both ground- and waterborne antennas need sharper beams and the capability to change directions at will (electronic scanning).

8.2 Displays

All displays of I information need improvement. The displaying of I information along with radar data on a radarscope provides an automatic correlation of targets, but the displays are confusing, and some make the I system subject to spoofing (Part 6.3.1.2). There is no suitable display available for airborne I information; a "Heads Up" display is needed. The Northrop Corporation, Palos Verdes, California, is now developing a flat, digitally addressed display that appears promising. The use of automatic decision devices, which are essential if FR and EA criteria are to be satisfied (Parts 6.2.7 and 6.2.8), requires better displays than those now available.

8.3 Detectors

Today's operational radar is woefully inadequate. Nonmilitary I functions can be performed without radar, provided the risks of collision with nonresponding aircraft can be tolerated. But radar is essential to nearly all military operations where identifications are made. Without good radar coverage to aid weapon delivery, there is little point in performing most of the military I functions described here.

Means of detecting and using enemy electromagnetic radiations are also very important. They should be a part of the CNI system but cannot be discussed here due to their high security classification (Part 7.1.2).

8.4 Data Processors

Data processors that are faster, smaller, lighter, more reliable, and less expensive are needed for the performance of both cryptographic and noncryptographic I functions. This fact, coupled with similar requirements for C and N functions, makes this a major problem area.

8.5 Signal Processors

It is abundantly clear that the performance of I functions requires signal processing techniques every bit as sophisticated as those required for the performance of C and N functions. The transition from current techniques to more efficient ones is particularly difficult. It now appears that both new and old techniques will have to be used simultaneously during the transition period, at least. This serves to make size, weight, power, etc., restrictions exceedingly severe.

8.6 Time Standards

It appears that all required military I functions can be performed with the time standards now available. However, many I functions, both military and nonmilitary, could be performed more efficiently if better standards were available, especially for use in mobile vehicles. Better time standards are certainly needed for C and N functions, too.

8.7 Concealment Techniques

Only a few of the possible techniques available for concealing our I transmissions from an enemy have been tried (25). The effective concealment of transmissions would, in principle, obviate the need for antijamming efforts. Even some relatively minor improvements in concealment capability might make jamming more difficult for an enemy.

8.8 Antijamming Techniques

Better antijamming techniques are always needed for I transmissions that an enemy can detect but cannot exploit. A continued effort on making I transmissions more difficult to jam is needed. Current I equipment does not make use of a number of well-known techniques that are being programmed for use in C equipment.

8.9 Collision Avoidance Techniques

The collision-avoidance problem for both military and nonmilitary aircraft has become a part of the nonmilitary I equipment's function by default. No one has found a way of solving the problem with radar or with simple C and N equipment. Current proposals for solution of the collision-avoidance problem (6,7,12) require very careful study, and probably considerable modification, before they will be acceptable.*

8.10 Reliability

Major improvements in equipment reliability are essential to the development and acceptance of any CNI system. System design must provide for a "graceful degradation" of functional performance in the event of failure rather than permitting a cataclysmic failure to occur.

8.11 Systems Analysis

The I of Neutrals, and Friends whose equipment fails (even partially), can be performed only by the use of astute operational procedures. The development of such procedures requires systems analysis of the highest order. Far too little effort has been spent thus far in determining all that can or might be done with available or to-be-available capabilities.

*A draft of the Report of the Department of Transportation Air Traffic Control Advisory Committee dated August 1, 1969 (not yet released for distribution) recently became available to the author. The suggestions in this report concerning how to handle air traffic and thus avoid collisions appear very promising.

9.0 SUMMARY AND CONCLUSIONS

This report provides a tentative, updated list of I requirements and describes some of the characteristics that a CNI system which satisfies them must have. It is concluded that a CNI system must be capable of performing both military and nonmilitary I functions (some of which could easily be interpreted as C or N functions) for all military services. The system must be designed to provide the I data needed by large ground and ship installations and by foot soldiers, as well as that required by aircraft. The I data for military users must be closely correlated with radar, or other sensor, outputs. No reason could be found for including satellite communication as an essential part of the system for I purposes, although there are cases where such communications would be convenient. Types of I systems are defined unambiguously in accordance with whether the identifier and/or the unidentified is active or passive, i.e. whether each sends messages or not, and whether electromagnetic radiation, when present, is essentially *omnidirectional* or limited to a relatively small *directive* angle. An evaluation of these *types* of I systems in accordance with how well each should be capable of identifying Enemies, Neutrals, and Friends reaches the following conclusions (see Table 2, p. 42):

1. Identifier Passive, Unidentified Passive (IPUP)

Systems of this type are useful only when all other means of I fail. (The Visual I system is of this type.)

2. Identifier Passive, Unidentified Active and Omnidirective (IPUAO)

This type of I system can be used for identifying enemies when the enemy produces recognizable signals; and it can be used for identifying friends in situations where identifier must remain undetected. (The TIFCO system (25) is of this type.)

3. Identifier Passive, Unidentified Active and Directive (IPUAD)

It may be possible to make some use of an enemy's directive radiations to identify him. This type of system is not suitable for identifying either neutrals or friends.

4. Identifier Active and Omnidirective, Unidentified Passive (IAOUP)

There are no practical I systems of this type.

5. Identifier Active, and Directive, Unidentified Passive (IADUP)

Systems of this type are of no value for *any* I function. Enemies can easily spoof all systems of this type if an attempt is made to identify enemies directly, and if the system is used to identify friends or neutrals, it can identify only a very limited number of types of vehicles and those only until an enemy captures, builds, or buys similar equipment. (The TRISAT system (29) is of this type.)

6. Identifier Active and Omnidirective, Unidentified Active and Omnidirective (IAOUAO)

Most C and N systems are of this type. They can provide some important I functions, but the data provided by them is more difficult to correlate with radar, or other sensor, information than that obtained by other types. This type of system can easily be made cryptosecure, and thus be free from enemy spoofing, and it offers one of the best means of identifying neutrals. The fact that it requires no equipment or techniques that are not also essential for C or N functions is important.

7. Identifier Active and Omnidirective, Unidentified Active and Directive (IAOUAD)

Systems of this type would offer no I capabilities that could not be provided more simply by other types. There are no existing or proposed systems of this type.

8. Identifier Active and Directive, Unidentified Active and Omnidirective (IADUAO)

This type of system provides I data that is exceedingly simple to correlate with radar data. It also is especially well suited for cryptographic techniques either with or without time synchronization. The directive identifier makes this type more difficult to jam than an omnidirective-identifier type would be. (The ATCRBS system now being used for air traffic control (5) and the Mark XII-TACIT system being developed for military use (31,35-38) are of this type.)

9. Identifier Active and Directive, Unidentified Active and Directive (IADUAD)

A system of this type would have numerous advantages over all others, but further research and development would be required in order to make such a system practical.

It is concluded that the Undersea category of I must be left out of current CNI efforts because the problem is too difficult to solve with current technology, not because there are no requirements for undersea identifications.

Finally, it is concluded that a properly designed CNI system offers the only real hope of identifying neutrals as well as friends and thus being able to consider the remaining unidentifieds as enemies. The only systems capable of identifying enemies directly are those that make use of the enemy's own radiation. Such systems are not always operable when needed.

10.0 RECOMMENDATIONS

This report should be considered only as a *start* toward clarification of the I requirements that a CNI system must satisfy. The author would appreciate receiving any comments or criticisms that readers may care to make.

11.0 ACKNOWLEDGMENTS

The author is indebted to Messrs. L. Higgins, E. Montalvo, and V. Terp of the Naval Electronics Laboratory Center, San Diego, California, for assistance in preparing the material in Part 2.1 of the report and for reviewing an early draft of the first five parts. He is also indebted to members of the Security Systems Branch for numerous criticisms and suggestions made during preparation of the report.

Table 1
The 25 Subcategories of I

Airborne, A	Space, S	Ground, G	Water, W	Undersea, U
AG†††	SG††	GG†††	WG†††	UG†
AW†††	SW††	GW†††	WW†††	UW†
AA†††	SA††	GA†††	WA†††	UA†
AS††	SS†	GS††	WS††	US†
AU†	SU†	GU†	WU†	UU†

†††Major subcategories: Must be included in CNI system.
††Supplementary subcategories: May be used in performing major subcategory functions - further study needed.
†Excluded subcategories: Excluded from current CNI studies due to lack of need or lack of capabilities.

Table 2
Types of Identification Systems

UNIDENTIFIED / IDENTIFIER		PASSIVE	ACTIVE	
			OMNIDIRECTIVE	DIRECTIVE
PASSIVE		IPUP (Part 5.1.1) Last Resort (Visual)	IPUAO (Part 5.1.2.1) EI, FI - Hidden Identifier (TEASER, TIFCO)	IPUAD (Part 5.1.2.2) (Null)
ACTIVE	OMNI-DIRECTIVE	IAOUP (Part 5.2.1) (Null)	IAOUAO (Part 5.2.2.1.1) NI, FI via C&N (All C & N Systems)	IAOUAD (Part 5.2.2.1.2) (Null)
	DIRECTIVE	IAOUP (Part 5.2.1) Unsafe for any I (TRISAT)	IADUAO (Part 5.2.2.2.1) FI, NI [AIMS (Mark XII: ATCRBS, Mark X (SIF), Mode 4 — TACIT)]	IADUAD (Part 5.2.2.2.2) FI, NI (Future Possibilities)

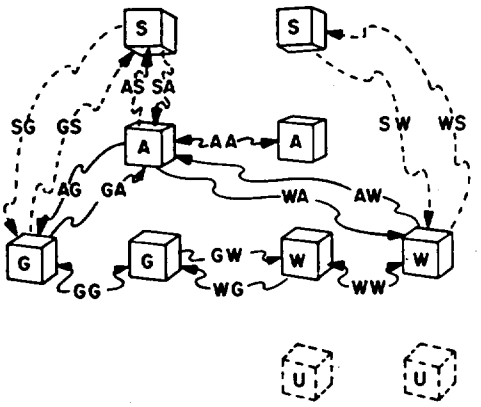

Fig. 1 - The nine major and six supplementary subcategories of identification

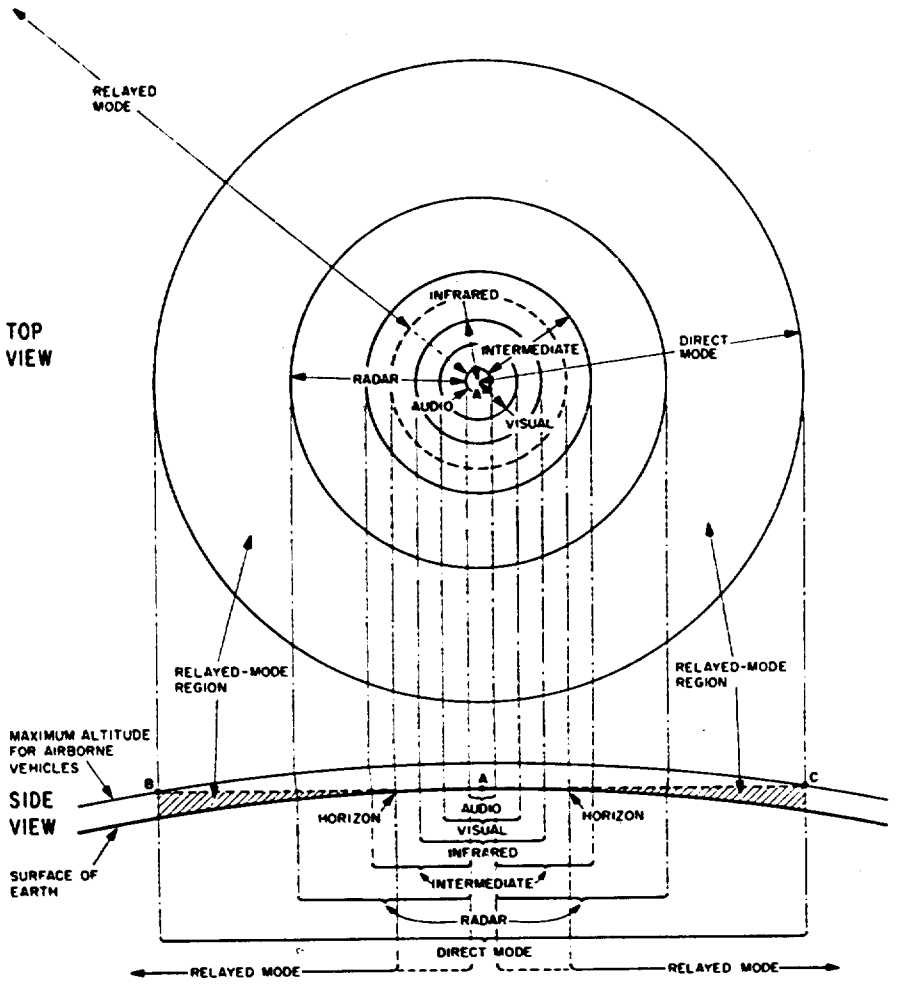

Fig. 2 - Identification ranges

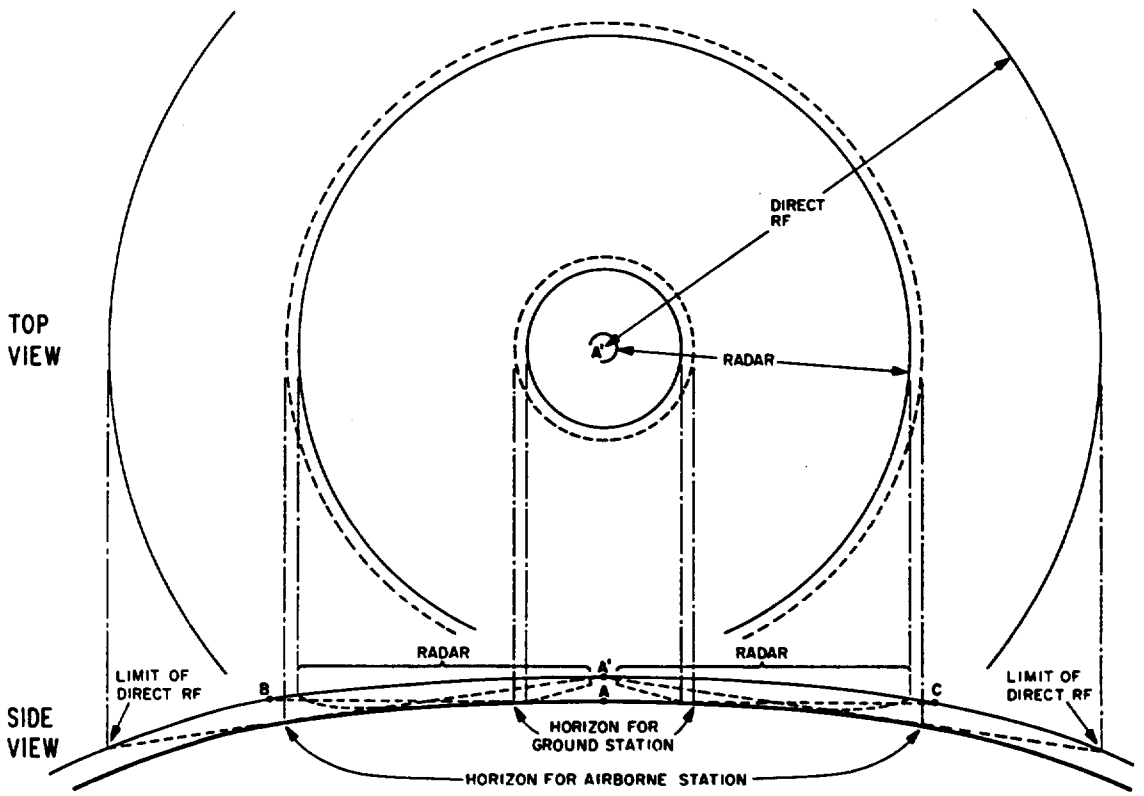

Fig. 3 - Airborne identification ranges

Nike Site*

The Army yesterday permitted a close look at the new Nike guided-missile station on Long Island in Boston Harbor, first of 12 around Greater Boston to be nearly completed. Once launching machinery has been installed, missiles can be fired from the elevator (center of upper picture) and from racks to be built on the platforms beside it. Newspapermen and photographers rode the huge elevator down into an underground storage vault (right picture) where missiles will be kept. A radar center to guide the electronically controlled Nikes is located at nearby Chapel Rocks, Squantum, on the other end of the Long Island causeway. Each of the 12 stations in the Greater Boston antiaircraft defense ring will be able to fire separately or in coordinated group action. There will be no firing practice at these sites, the Army said. Nike missiles reportedly can outmaneuver present-day planes. Six missiles can be kept on the side racks at all times, while two can be fired from the elevator.

To Shoot or Not to Shoot Worries Pilots at Cape Base**

A youthful pilot here disclosed a hitherto untold angle of night time flights. Day flights are not so difficult. But there's a special wrinkle at night. He said:

"Say you are sent out on a course that will lead you to an 'unknown' approaching at 20,000 feet.

HAND FLASHLIGHT USED ON MARKINGS

"It's dark, so you have to edge in and fly along side the stranger to make identification. So you can't see, and you have to dig out a hand flashlight and play the beam along the other airplane until you can read its markings.

"I predict that the first dead heroes of a shooting war around here will be the crew of one of our planes.

"This is because they'll be sitting ducks, working that flashlight, if it happens to be an enemy bomber.

"Every time a jet crew swings in close at night, this knowledge is riding with them."

After that, he explained it will just be a question of whether the first jet's wingman can get the bomber—or be clobbered in turn.

FRIEND OR FOE ?

(FLASHLIGHT IDENTIFICATION SYSTEM)

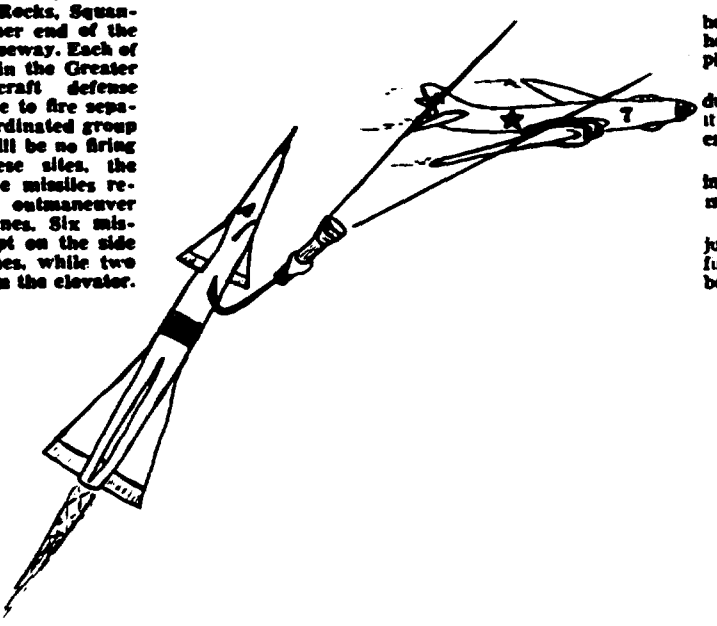

Fig. 4 - The fallacy of weapon capability without I capability

*From The Christian Science Monitor © 1955 The Christian Science Publishing Society. All rights reserved.
**From the Boston Herald Traveler, Feb. 8, 1955.

REFERENCES

NOTE: Page numbers in parentheses are those text pages on which the subjects are discussed.

1. Parker, C.V., "Cooperative Functions in Communication, Navigation, and Identification," NRL Report 5300 (Secret Report, Unclassified Title), May 12, 1959 (p. 1)

2. Cleeton, C.E., "Proposed System of Electronic Recognition," NRL Report 3131 (Secret Report, Unclassified Title, June 1947 (pp. 2, 12)

3. Bishop, W.B., and LaRochelle, J.A., "IFF Security Proposal by the Communications Laboratory," AFCRL, Hanscom AFB (Secret Report, Unclassified Title) May 20, 1954 (pp. 2, 12)

4. Operational Requirement AD-02401 (Revised) IFF Capability; Enclosure 4 to OPNAV-INST 002380.1A (Secret Document, Unclassified Title) Oct. 28, 1958, (pp. 2, 12, 37)

5. "U.S. National Standard for the IFF Mark X (SIF) Air Traffic Control Radar Beacon System (ATCRBS) Characteristics," (Unclassified) Oct. 10, 1968 (pp. 3, 4, 11, 22, 29, 36, 41)

6. "McDonnell-Douglas Aeronautics Company EROS (Elimination of Range Zero System)," The McDonnell Collision Avoidance Concept Report No. A502, (Unclassified) Feb. 7, 1964 (pp. 4, 39)

7. Bluin, J.E., and Phillips, F.M., "Collision Avoidance System," McDonnell-Douglas Astronautics Co., Eastern Division, St. Louis, Mo.; prepared for Airlines Electronic Engineering Committee, Collision Avoidance System Subcommittee Meeting, (Unclassified) Aug. 12, 1969 (pp. 4, 39)

8. Report by the USAF Scientific Advisory Board Ad Hoc Committee on Air-by-Air IFF (Secret Report), Apr. 11, 1966 (pp. 10, 33)

9. Klass, P.J., "Air Traffic Control Blueprint," Aviation Week and Space Technology, Jan.-Feb. 1964 (p. 10)

10. Swerling, P., "Lecture Notes on Radar Target Signatures: Measurements Statistical Models and Systems Analysis," Technology Service Corporation, Santa Monica, Calif. (one-week lecture course given at NRL in May 1969), Aug. 1968 (p. 19)

11. Lawson, J.L., "Detection of Propeller and Sambo Modulations," Radiation Laboratory Report (S-10), M.I.T., May 16, 1944 (pp. 19, 34)

12. Alexander, B., "Department of Transportation Air Traffic Control Committee Report," General Research Corporation, Santa Barbara, Calif., EASCON 1969 Convention Record, Oct. 1969 (pp. 22, 36, 39)

13. Sturtevant, J.L., "Range of Rotating Corner Reflector Ship Identification," Radiation Laboratory Report 103, M.I.T., July 7, 1943 (p. 25)

14. Sturtevant, J.L., "Rotating Corner Reflectors for Ship Identification," Radiation Laboratory Report 654, M.I.T., Jan. 1, 1945 (p. 25)

15. Stockman, H., "Communications by Means of Reflected Power," Proc. IRE 36:1196-1204 (Oct. 1948) (p. 25)

16. Bishop, W.B., "The Practicability of Retrodirective Reflectors for Communications Purposes," Report E4081, Air Force Cambridge Research Center Laboratories, Cambridge (now L.G. Hanscom Field), Mass., (Unclassified), June 1951 (pp. 25, 37)

17. Leland, T., "Now Can Send Voice on Beam of Light," The Boston Sunday Globe, Apr. 19, 1964 (p. 25)

18. Addendum to the Joint Military Characteristics of the IFF Mark XII (submitted by the National Security Agency in March 1965) (p. 29)

19. Bishop, W.B., "A Semiautomatic Jam-Accept (SAJAC) Decider for Mode 4 of the IFF Mark XII," NRL Report 6751 (Confidential Report, Unclassified Title), Oct. 11, 1968 (pp. 29, 31, 36)

20. Cleeton, C.E., "Coding and Security of Electronic Recognition and Identification Systems," (Secret Report, Unclassified Title) Sept. 12, 1946 (p. 30)

21. Parker, C.V., "Some Possible Enemy Countermeasures to IFF," NRL Letter Report S-5260-61A/54dd (Secret Report, Unclassified Title), July 22, 1954 (p. 31)

22. Parker, C.V., "Another IFF Countermeasure: Repeating Interrogations," NRL Letter Report S5260-79A/54dd Ser 1609 (Secret Report, Unclassified Title), Sept. 22, 1954 (p. 31)

23. Bishop, W.B., "The Failure-Indicating Module," Proc. Second Annual Joint Military-Industrial Electronic Test Equipment Symposium, Washington, D.C., Vol. I, pp. 47-73 (prepared by Project SETE, New York University, SETE 230/2.1) (p. 32)

24. "Development Guidance for Identification Systems," OPNAV 00217P72 (Secret Report, Unclassified Title), Aug. 14, 1967 (pp. 33, 34)

25. Higgins, L.N., "NEL TIFCO Project, Phases 1 and 2," Navy Electronics Laboratory Report 1327 (Secret Report, Unclassified Title), Nov. 2, 1965 (pp. 33, 39, 40)

26. Makinson, H.O., Crispell, H.L., Edge, A.D., and Gustafson, J.B., Lt. USNR, "TIFCO-LPI-CNI System: Operations Analysis," NELC Report 1565 (Secret Report, Unclassified Title), Sept. 18, 1968 (p. 34)

27. Dawirs, W.R., and Miyashiro, S.K., "Low-Intercept-Susceptibility Air-Navigation System (LISANS) — TIFCO Version," NELC Report 1592 (Secret-NOFORN Report, Unclassified Title), Oct. 23, 1968 (p. 34)

28. Higgins, L.N., and Dawirs, W.R., "TIFCO-LISANS Systems Flight Tests," NELC Report 1641 (Secret Report, Unclassified Title) Nov. 19, 1969, (p. 34)

29. Short, E.P., "TRISAT Acceptance Test," NWC TP-4579 (Secret Report, Unclassified Title), June 1968 (pp. 34, 35, 40)

30. "Radio Navigation Systems for Aviation and Maritime Use," W. Bauss, Technical Editor, New York:Pergamon Press, 1963 (p. 35)

31. "Mark XII IFF Operational Test and Evaluation Final Report," ESD-TR-61, U.S. Air Force, U.S. Army, U.S. Navy, and U.S. Marine Corps (Secret C/CNR Report, Unclassified Title), Nov. 1961 (pp. 35, 36, 41)

32. "Study to Provide Integrated Anti-Jam Navigation, Data-Link, and IFF System in the TACAN Spectrum," Final Engineering Report on Contract NObsr-77551, Index No. NE-010200 by ITTF Laboratories (a division of International Telephone and Telegraph Corporation, Nutley, N.J.) (Secret Report, Unclassified Title), Jan. 1961 (p. 35)

33. Dawirs, W.R., "Integrated CNI (Communication, Navigation and Personal Identification)," NELC Report 1064 (Confidential Report, Unclassified Title) (p. 35)

34. Bishop, W.B., "IFF Mark XII Timing Sequences," NRL Memorandum Report 1819 (Confidential Report, Unclassified Title), Sept. 25, 1967 (p. 36)

35. "DOD AIMS System Package Program," Air Force-Army-Navy-NSA for ATCRBS/IFF/ Mark XII Systems, by DOD AIMS System Program Office, Deputy for Systems Management, Aeronautical Systems Division, Wright-Patterson AFB, Ohio (Secret Report, Unclassified Title), Feb. 15, 1967 (pp. 37, 41)

36. Hovey, J.M., and Parker, C.V., "Mark XII IFF System Authentication," NRL Report 6264 (Secret Report, Unclassified Title), May 1965 (pp. 37, 41)

37. Hovey, J.M., "The NRL TACIT Project," NRL Report 6569 (Secret Report, Unclassified Title), Feb. 1967 (pp. 37, 41)

38. Hovey, J.M., "Authentication of the SIF Modes of the Mark XII IFF System," NRL Report 6882 (Secret Report, Unclassified Title), Mar. 1969 (pp. 37, 41)

☆ U.S. GOVERNMENT PRINTING OFFICE: 1970-397-176/138

Unclassified
Security Classification

DOCUMENT CONTROL DATA - R & D
(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)	2a. REPORT SECURITY CLASSIFICATION
Naval Research Laboratory Washington, D.C. 20390	Secret - NOFORN
	2b. GROUP 3

3. REPORT TITLE

THE I OF CNI: SOME IDENTIFICATION PROBLEMS AND THEIR RELATION TO COMMUNICATIONS AND NAVIGATION

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

An interim report on one phase of a continuing problem.

5. AUTHOR(S) (First name, middle initial, last name)

Walton B. Bishop

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
April 23, 1970	54	38

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
NRL Problem R01-45 b. PROJECT NO. A36533/652/69F15-222-602 c. d.	NRL Report 7033 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEME[redacted]

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Department of the Navy (Naval Air Systems Command), Washington, D.C. 20360

13. ABSTRACT

(Unclassified)

The military and civilian requirements for identification are examined to determine what sort of communications and/or navigation techniques may, or might, be used to satisfy them. A tentative updated list of identification requirements and a draft of characteristics that an electronic system needs in order to satisfy them are provided.

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Communication, Navigation, and Identification (CNI) functions Identification Recognition IFF						

UNITED STATES GOVERNMENT

memorandum

5300-040

DATE: 24 August 1998

REPLY TO ATTN OF: Code 5300

SUBJECT: REQUEST TO DECLASSIFY NRL REPORTS

TO: Code 1221.1 (C. Rogers) On 11/20/98

1. It is requested that the NRL Reports listed below be declassified. The information contained in these reports has become public knowledge in the many years since first classified.

Declassify, public release.

✓2138 ✓5790 [redacted] [redacted] ✓7033

✓5694 ✓5821 [redacted] [redacted]

✓5755 [redacted] [redacted] ✓5876

Declassify, DoD and DoD contractors only. These Reports contain Critical Technology.

✓5636

[redacted]

✓5835

Edward E. Maine

EDWARD E. MAINE
Associate Superintendent
Radar Division